



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

OCIO POLICY FOR ENTERPRISE CONFIGURATION MANAGEMENT PLANS OCIO-5011-09

Date of Issuance: September 23, 2009

Effective Date: September 23, 2009

Review Date:

TABLE OF CONTENTS

Section

- I. Purpose
- II. Scope
- III. Definitions
- IV. Policy
- V. Roles & Responsibilities
- VI. Compliance and Management Commitment
- VII. Effect on Other Policies

Appendix A – Suggested Table of Contents for Organizational Configuration Management Plans

I. PURPOSE

This purpose of this policy is to provide guidance for the development of Organizational Configuration Management Plans for agency software applications and infrastructure that will provide the basis of an Enterprise Configuration Management Program for the USPTO. Organizational CM plans will constitute the basis for continuity of operations planning in a disaster situation. It is a companion to agency COOP and BCDR artifacts.

The purpose of an Organizational CM Plan is to identify artifacts, processes and procedures critical to a business unit and detail how those critical items will be controlled and managed over time; assuring continuity of operations for USPTO business functions, regardless of staff turnover, tools evolution or more critical business interruptions.

II. SCOPE

The Enterprise Configuration Management Policy relates to all of the OCIO organizations that will need to function in response to a disaster. In addition to the IT Infrastructure, this policy covers financial, HR, procurement and contracting organizations as well as the customary application development organization. Resumption of administrative and support activities will be equally as critical as technical operations to the OCIO, to recover from a disaster.

OCIO Policy for Enterprise Configuration Management Plans

The scope of this Policy is not to prescribe what business artifacts and metadata need to be captured in the configuration management repository, rather this Policy provides guidance about the nature of a CM Plan. The CM plan needs to identify artifacts that will likely be needed to assist a team of IT professionals *not* familiar with the USPTO business, to reconstitute the business environment and applications and recover the production environment at an alternate processing site following a disaster. Ultimately, the business organization will need to identify the relevant CM artifacts for its operation to continue to function and develop the procedures and discipline to ensure that they are followed. This policy will not prescribe an absolute set of artifacts to be configuration managed by the OCIO.

It is the responsibility of the business director to determine the key business artifacts, processes and procedures and work with Enterprise CM staff to define configuration items, determine the most effective means for controlling and recovering the CIs, and institute policies and procedures for authorizing changes.

III. DEFINITIONS

Following are fundamental CM terms that will help define and guide the content of an Organizational CM Plan.

Authoritative Source – An organization’s universally recognized source for a specific piece of business information. The authoritative source may be a specific database, a specific COTS product, a web-link or any other media, including a human being. The form is immaterial; the key is that the organization recognizes the “truth” of the authoritative source and the source is singular in nature. Retaining the integrity of an authoritative source is one of the goals of configuration management.

Baseline – A “snapshot” of a configuration item(s) at a specific point-in-time when it is considered complete and viable. A Production Baseline refers to the set of fully vetted CIs that are used to conduct today’s business.

Change Management – A prescribed discipline, by which changes to configuration items are identified, designed/developed, approved and implemented to create a new baseline for a CI.

Configuration Control – A set of processes and approval stages required to change a configuration item's attributes and to re-baseline the CI. Configuration Control is the result of effective change management.

Configuration Identification – The process of identifying the artifacts and attributes that define every aspect of a configuration item that is essential for a business unit to function.

Configuration Item (CI) – A configuration item is an artifact that has a substantive business purpose. It can be software code, network settings, hardware inventories, a spreadsheet, a set of metadata, a COTS product, SOPs, policies, job aides; any concrete item that is essential for the ongoing viability of a

business unit. Attributes of a CI can also be considered a CI, if they change over time to reflect evolving business requirements.

Configuration Management Data Base (CMDB) – In the ITIL context, a CMDB is a federation of repositories that are managed by a dedicated CM organization and contain the authoritative sources of CIs for the organization.

Configuration Management & Planning – The process of developing a strategy for assuring business continuity for an organization using principles that produce structured and repeatable processes to retrieve critical artifacts from which to rebuild a business unit and ultimately, an organization.

Configuration Status Accounting – Configuration status accounting is the discipline to record and report on configuration baselines at any moment in time. Status Accounting assumes that the authoritative source of a CI is clearly understood by the organization and tracked and managed accordingly.

Configuration Verification and Audit – Configuration audits are broken into functional and physical configuration audits. Audits occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is implemented in accordance with the requirements of its detailed design documentation.

Information Technology Infrastructure Library (ITIL) – A framework of concepts, techniques, and best practices for managing information technology (IT) infrastructure, development, and operations.

IV. POLICY

All organizations, headed by a Senior Executive Service (SES) Executive, shall maintain a Configuration Management Plan (or plans if applicable) to address application and infrastructure recovery to ensure continuity of operations in the event of a disruption in business. An Organization's Configuration Management Plan will align with this policy, be approved by the OCIO, and be reviewed on an annual basis to ensure that it reflects current business practices. (A suggested table of contents is contained in Appendix A of this Policy for an Organizational CM Plan.)

V. ROLES & RESPONSIBILITIES

Each SES Group Director within OCIO will maintain a Configuration Management Plan(s) that supports continuity of operations for his/her organization. The Enterprise Configuration Management Division (ECMD) will assist the development of organizational CM Plans; however, the breadth and depth of the organization's configuration items will be determined by the business organization, not prescribed by ECMD. This may be accomplished by a standing committee of key organizational managers, or assigned to a Configuration Management Coordinator by the SES.

OCIO Policy for Enterprise Configuration Management Plans

It is the responsibility of ECMD to provide assistance automating the business area CM Plan, so that the configuration items identified by the business area will be properly managed, backed up, and retrievable under a disaster scenario. ECMD will provide CM tool administration, and work closely with each business area during definition and implementation of processes and procedures to manage user access and IDs, capture CIs and manage them effectively through change management.

The SES Executive shall review the CM Plan Annually to ensure that it remains a viable plan for recovering his/her business unit.

VI. COMPLIANCE AND MANAGEMENT COMMITMENT

Compliance with the OCIO Policy on Enterprise Configuration Management will be assessed on an annual basis through the issuance of a *State of ECM Report* produced by ECMD and delivered to the OCIO SES Executives during the third quarter of each Fiscal Year. This report will provide:

1. A comprehensive assessment of the maturity of both individual business unit plans and overall OCIO preparedness to handle a major disaster, and
2. Recommendations to improve ECM across the OCIO.

Management's commitment to this policy will be reflected in annual performance ratings of OCIO's SES-level management based on the results of implementing a configuration management discipline within their respective organizations. *The State of ECM Report* will provide input for this performance assessment.

VII. EFFECT ON OTHER POLICIES

This Policy does not affect any other policies. It forms the basis for responding to Agency COOP and BCDR initiatives, which address the global, agency-wide continuity scenario.

ISSUED BY:

Issued By: John B. Owens II, CIO USPTO
(Signature)

John B Owens II
Chief Information Officer
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: Office of Information Management Services

Appendix A

Suggested Table of Contents for Organizational Configuration Management Plans

| | | |
|------------|--|------------|
| 1.0 | INTRODUCTION | 1-1 |
| 1.1 | Purpose | 1-1 |
| 1.2 | Scope | 1-2 |
| 1.3 | Applicable Documents/Policy Directives | 1-3 |
| 2.0 | ORGANIZATION AND FUNCTIONS | 2-1 |
| 2.1 | Organization Overview of Services | 2-1 |
| 2.2 | Roles and Responsibilities | 2-2 |
| 2.2.1 | Division/Branch #1 | 2-3 |
| 2.2.2 | Division/Branch #2 | 2-4 |
| 2.2.3 | Division/Branch #3 | 2-5 |
| 2.2.4 | Division/Branch #n | 2-6 |
| 2.3 | Configuration Management Decision Authorities | 2-7 |
| 2.3.1 | Organizational CM Assumptions and Interdependencies | 2-8 |
| 2.3.2 | Organizational Change Control and Interdependencies | 2-9 |
| 2.4 | Contractor Implications/Considerations | 2-10 |
| 3.0 | CONFIGURATION IDENTIFICATION | 3-1 |
| 3.1 | Operational Concept of Operations | 3-1 |
| 3.1.1 | Pre-requisites for Operational Continuity of Service | 3-2 |
| 3.1.1.1 | Facility Requirements (Minimum and Optimal) | 3-3 |
| 3.1.1.2 | Staffing Requirements (Minimum and Optimal) | 3-4 |
| 3.1.1.3 | Hardware, Software and Supplies (Minimum and Optimal) | 3-5 |
| 3.1.2 | Continuity Priorities | 3-6 |
| 3.1.3 | Dependencies with other Organizations | 3-7 |
| 3.2 | Strategy for Defining Configuration Items | 3-8 |
| 3.2.1 | Organizational CIs | 3-9 |
| 3.2.2 | Cross-organizational CIs | 3-10 |
| 3.2.3 | Roles and Responsibilities for ongoing CI Identification | 3-11 |
| 3.2.4 | CI Matrix | 3-12 |
| 3.2.5 | Definition of Terms | 3-13 |

| | | |
|------------|--|------------|
| 4.0 | INTERFACE MANAGEMENT | 4-1 |
| 4.1 | Interface with Enterprise CM Division | 4-1 |
| 4.2 | Interface with other organizations that impact CM | 4-2 |
| 5.0 | CONFIGURATION CONTROL | 5-1 |
| 5.1 | Configuration Control Documentation and Processes | 5-1 |
| 5.1.1 | Organizational Change Management | 5-2 |
| 5.1.1.1 | Request for Change | 5-3 |
| 5.1.1.2 | Change Control Board | 5-4 |
| 5.1.1.3 | Process for approved changes | 5-5 |
| 5.1.2 | Interfaces with OCIO Change & Configuration Management | 5-6 |
| 5.1.3 | Interfaces with DoC Change Management (if applicable) | 5-7 |
| 6.0 | CONFIGURATION STATUS ACCOUNTING | 6-1 |
| 6.1 | Strategy for Monitoring Currency of Organizational CIs | 6-1 |
| 6.2 | Available Reports of CI States | 6-2 |
| 6.3 | Key Performance Indicators of Successful Organizational CM | 6-3 |
| 7.0 | CONFIGURATION AUDITS | 7-1 |
| 7.1 | Design and Document Verification | 7-1 |
| 7.2 | Audit Prerequisites | 7-2 |
| 7.3 | Continuing Performance Audits and Surveillance | 7-3 |
| 7.4 | Design Reviews | 7-4 |
| 7.5 | Conduct of Reviews/Audits | 7-5 |
| 8.0 | SUPPORT CONTRACTOR CMP | 8-1 |
| 8.1 | Overview of Organization’s Contracting Activities | 8-1 |
| 8.2 | Strategy for assuring Contracting Activities support Organizational CM | 8-2 |
| 8.3 | Specific Contract Terms and Conditions relative to CM | 8-3 |
| 8.4 | Impacts of Non-Compliance | 8-4 |
| 8.4.1 | Organizational Impacts for Contractual non-compliance | 8-5 |
| 8.4.2 | Contractual remedies for non-compliance with Organization’s CM Plan | 8-6 |

LIST OF FIGURES

| | | |
|-------------|---|-----|
| Figure 2-1: | Flow of activities for Organizational CI Change Control | 3-9 |
| Figure 3-1: | Flow of activities with Enterprise Configuration Management | 5-6 |

LIST OF TABLES

| | |
|---|------|
| Table 3-1: Matrix of Organizational Configuration Items | 3-12 |
|---|------|

APPENDIX

| | |
|--|-----|
| Appendix A: List of Acronyms and Abbreviations | A-1 |
|--|-----|