DEFENSE PERSONAL PROPERTY SYSTEM (DPS)

Configuration Management Plan

MILLER.MICHAEL.J.1152
974660

Digitally signed by MILLER.MICHAEL.J.1152974660
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USAF, cn=MILLER.MICHAEL.J.1152974660
Date: 2011.04.29 12:37:52 -05'00'

MICHAEL J. MILLER, Colonel, USAF
Prog Director, JPMO Household Goods Systems (HHGS)
and Deputy, Program Executive Officer
Acquisition Directorate, USTRANSCOM

15 April 2011
Version 2.0

Table of Contents

List of Tables

Table of Figures

Table 1 Document Change History

Version	Date	Changes
1.1	24 Sep 10	Initial draft using USTRANSCOM PMO CMP Template 3.0
1.14	4 April 2011	Made changes resulting from multiple DPS reviews.
2.0	15 April 2011	Version 2 Deliverable

1 Introduction

The Configuration Management (CM) discipline is applied to controlled items for which the project organization has development and/or maintenance responsibilities. The CM organization implements the activities described within this plan to ensure that controlled products and controlled activities are compliant with governing policies and procedures and that changes are correct and appropriately managed.

CM ensures that changes take place in an identifiable and controlled process and do not adversely affect any properties of the system, other systems, or interfaces. CM provides a detailed methodology for controlling design and development throughout the lifecycle of today's complex systems.

1.1 Purpose

The purpose of this Configuration Management Plan (CMP) is to provide overall CM guidance and direction to establish uniform procedures to control system change initiatives with the objective of coordinating, controlling, approving, and auditing changes. Successful CM requires that CM processes, procedures, and responsibilities be established early in program life-cycles. Effective CM requires support from senior management, adequate training for personnel responsible for CM, and a conceptual understanding of CM by all involved, and individual and organizational discipline to follow CM procedures.

This CMP provides policies and procedures to identify, control, and audit the functional requirements and technical characteristics of the Defense Personal Property System (DPS) implementation efforts. The Joint Program Management Office (JPMO) Household Goods Systems (HHGS) CMP addresses:

- Formal CM and administrative procedures to allow the DPS Configuration Working Group (CWG) and Functional Requirements Board (FRB) and Configuration Control Board (CCB) members, to identify, control, and document changes
- Administrative CM procedures, status accounting, CM audits, change control and baseline control CCB processes, tasks, and responsibilities
- Life-Cycle Management (LCM) CM milestones that address schedule, cost performance and program direction
- CM change request processes that document problems, implement solutions, and control system evolution. A CM change is defined as anything that affects cost, schedule, or performance. This CMP will assist the DPS CCB in controlling change through CM baselines by achieving the following goals:
  - Ensure functional and system requirements (needs) are met.
  - Ensure all changes are tracked, controlled, approved, monitored, and managed throughout lifecycles.
  - Ensure Department of Defense (DOD) technical standards are met.
  - Ensure that each change request or recommendation is evaluated for functional, operational, technical, security and economic impact on the entire system before the change is validated and implemented.

This CMP describes the CM organization and practices applied throughout the life of the DPS program on controlled products and activities that are developed, executed and maintained for the United States Transportation Command (USTRANSCOM) Program Management Office (PMO).

1.2 System Overview

Each year, the Department of Defense (DOD) moves more than 600,000 shipments per year for Service members and civilians, at a cost of over $2 billion per year. Over 76% of personal property shipped is through Defense Personal Property Program (DP3). Surface Deployment and Distribution Command (SDDC) manages DP3 for the DOD. A total of 151 DOD and Coast Guard Personal Property Shipping Offices (PPSOs) manage shipments and 961 Transportation Service Providers (TSPs) provide moving and storage services.

TOPS is scheduled to be sunseted in the future but is still in use at this time. DPS is a single, end-to-end, web-based solution for personal property shipping. In 2007, the United States Transportation Command (USTRANSCOM) stood up the Joint Program Management Office (JPMO) Household Goods System (HHGS) to assume the DPS program management responsibilities.

DPS provides a single, centralized, Web-based system for the management of personal property shipments for the DOD. The system is responsible for all aspects of personal property management, including:

- Qualification of Transportation Service Providers (TSP)
- TSP Rate Filing and Acceptance
- Counseling
- Customer Satisfaction Survey
- Shipment Management
- Best Value Scoring (BVS)
- TSP Ranking
- Printing of Standard Forms
- User Management and Security
- Shipment Costing, Invoicing, and Approvals
- Claims
- External Interfaces
- Reports
- Tracking and Audit Trail
- Two-dimensional Military Shipping Labels (2DMSL)
- Personal Property Consignment Instruction Guide (PPCIG)
- Learning Management System (LMS)
- Interactive Voice Recognition (IVR)
- Access to the TOPS System

DPS is composed of a number of distinct software components, consisting of Commercial Off-the-Shelf (COTS) components such as Siebel® and Manugistics®, Government Off-the-Shelf (GOTS) components, and Java 2 Enterprise Edition (J2EE)-based custom code that, when combined, implement specific business logic/requirements. All non-Siebel components are J2EE-based and run under the Oracle WebLogic Application Server using the standard 3-tier architecture approach of J2EE.

DPS utilizes a centralized database to interface with other Government systems, including the Third Party Payment System (TPPS) and provides management reports, as well as electronic shipment documentation to TSPs participating in the program.

1.3 Document Overview

This CMP describes the DPS program approach to the configuration management and control of hardware, software, and documentation. This plan focuses on the Government CM activities to include data management, configuration identification, change control, status accounting, and configuration audits of the DPS CM activities and program products. The contractor's CM Plan and this plan are complementary, each detailing a different part of the whole CM process for this project.

Section one of this CMP contains general introductory information.

Section two lists the References.

Section three describes the CM Organization and Concept of Operations.

Section four discusses Data Management.

Section five discusses the CM processes.

In the event of conflict between this plan and other documents referenced herein, the documentation requirements of this plan shall apply. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

1.4 Scope

At a minimum, this plan will be reviewed annually, and updated as required. This plan is in effect until DPS has been retired or this plan has been rescinded by the Program Manager (PM).

1.5 Terms and Abbreviations

Appendix A lists the terms and abbreviations appropriate to the DPS Program and used in this document.

2 References

The following documents serve as guidance for this CMP and are listed in order of precedence.

- MIL-HDBK-61A (SE), Configuration Guidance, 7 Feb 2001
- Capability Maturity Model Integration for Systems Engineering/Software Engineering/ Integrated Product and Process Development V1.2.

The following is a list of documentation referenced in this CMP.

- Government documents:
  - DPS Requirements Management Plan (RMP) v1.0
  - DPS Test and Evaluation Master Plan 1.0
  - DPS CCB Charter v1.0
  - DPS System Change Request Form Appendix B
  - DPS CCB Minutes Template Appendix C
- Developer documents:
  - CMP v4.0

This plan complies with standard DOD CM regulations, standards, and directives. As changes are made to the following governing documents, this plan will be modified accordingly:

- DOD Regulation 5000.2-R directs in paragraph C5.2.3.4.5:

  The PM will ensure that the systems engineering process will provide, among other things, “A configuration management process to guide the system products, processes, and related documentation, and to facilitate the development of open systems. The configuration management effort includes identifying, documenting, and auditing the functional and physical characteristics of an item; recording the configuration of an item; and controlling changes to an item and its documentation. It shall provide a complete audit trail of decisions and design modifications.”

- DOD Directive 8000.01 directs in paragraph 4.4.5:

  A “disciplined life-cycle approach to manage information resources from acquisition through retirement.”

- DOD Instruction 8500.2, paragraph E3.3.8:

  “strong configuration management is a foundation requirement for successful vulnerability management, and the two functions shall be highly coordinated.”

- DOD Instruction 8500.2, IA Control DCPR-1:

  “a configuration management process is implemented that includes requirements for:

  (1) formally documented CM roles and responsibilities

  (2) a configuration control board that implements procedures to ensure a security review and approval of all proposed DOD information system changes, to include interconnections to other DOD information systems;

(3) a testing process to verify proposed configuration changes prior to implementation in the operational environment; and

(4) a verification process to provide additional assurance the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted."

- CJCSI 6212.01D Interoperability and Supportability of Information Technology and National Security Systems, Table D-4: "all providers of services on the Global Information Grid (GIG) will "Adhere to enterprise configuration management" of key interfaces."

3 CM Organization and Concept of Operations

3.1 CM Organization

Figure 1 shows the matrix structure of the JPMO organizational chart. Configuration Management resides in the Engineering Support and supports the DPS program and the PM.

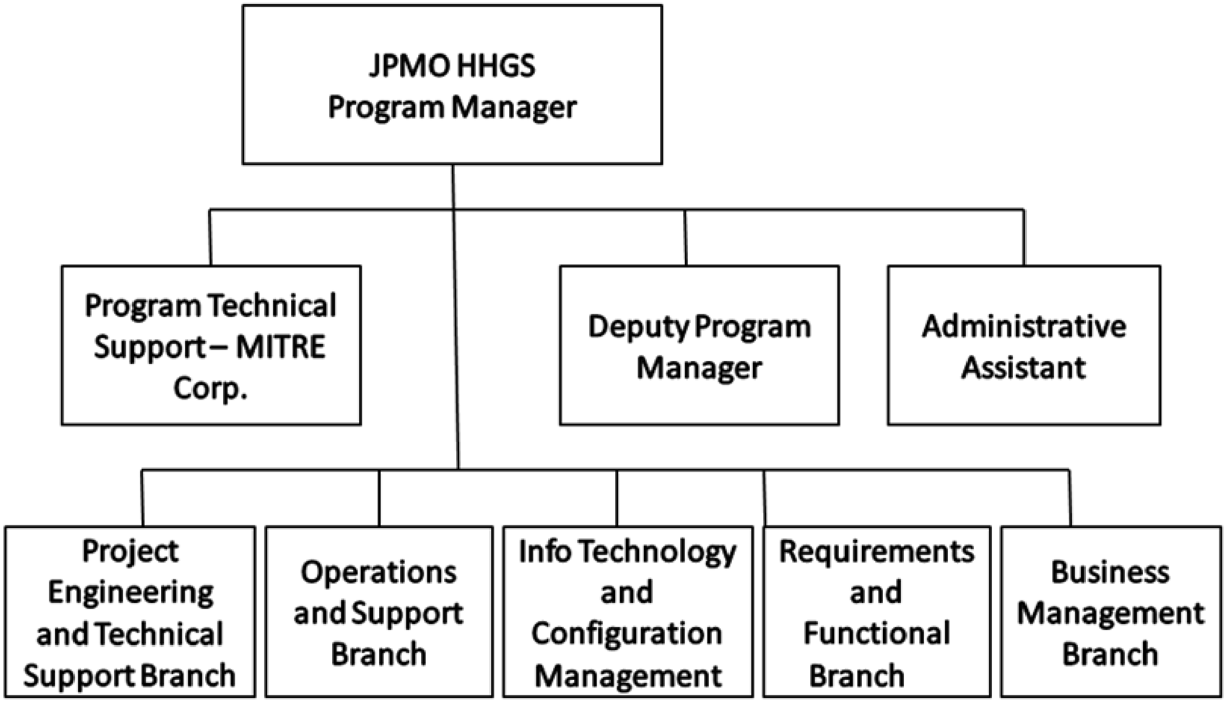
JPMO HHGS
Program Manager
Program Technical Support – MITRE Corp.
Deputy Program Manager
Administrative Assistant
Project Engineering and Technical Support Branch
Operations and Support Branch
Info Technology and Configuration Management
Requirements and Functional Branch
Business Management Branch

Figure 1 JPMO Organizational Chart

The USTRANSCOM PMO CM team provides oversight to the contractor's CM. The DPS CM is supported by the USTRANSCOM PMO CM team.

3.2 CM Concept of Operations

This CMP is designed to assist the DPS PM to:

- Establish and maintain a configuration management system and change management system for controlling work products
- Monitor the status and content of the system configuration
- Support the established product baselines
- Monitor the status of the product baseline
- Track and control changes; efficiently manage changes to the system configuration and product baselines to include documentation
- Track and control changes to contractual and non-contractual documents and artifacts
- Establish integrity; control the integrity of the system configuration and product baseline
- Establish CM records

The following CM practices and procedures will be applied to the DPS program:

- Configuration changes shall be tracked and controlled throughout the life cycle of DPS.
- CM implementation will be consistent with the objectives of the DPS program and its complete life-cycle management milestones and phases.

- Changes to DPS shall be made expeditiously with the least disruption and with best value.
- The DPS CCB is responsible for the CM policies and procedures and the CCB representatives are responsible for their specific CM requirements.

4 Data Management (DM)

Data management comprises all the disciplines related to managing data as a valuable resource. This includes receiving, storing, reviewing, maintaining, updating, controlling, and being able to retrieve data.

The PMO CM is responsible for data management for the PMO documentation and program documentation including both contractual and non-contractual data.

4.1 Library

The USTRANSCOM PMO CM team provides an electronic library database for all documentation. This library contains contractual and non contractual data deemed important to the USTRANSCOM PMO and/or individual programs. CM provides document control in the library managed by limited access for data defined sensitive by the Program Director or PM.

The USTRANSCOM PMO Configuration Manager is responsible for all data management information in the USTRANSCOM PMO CM database (library). The database will contain but will not be limited to the conceptual, logical, and physical data models used in DPS and future personal property systems, USTRANSCOM PMO documentation and program documentation including both contractual and non contractual data.

4.1.1 Contractual Data

Contractual data includes all deliverables of documentation and source code delivered by the program's development contractor. This data will be provided to CM via the CM mailbox at USTCJ6-P-CM@USTRANSCOM.MIL. Typical documents that fall into this category include, but are not limited to:

- Functional Requirements Documents
- Design Documents
- Interface Documents
- Test Documents
- Version Description Documents
- Manuals and Guides
- Database Documents
- Statements of Work
- Contract Modifications
- Status Reports
- Source Code

4.1.2 Non-Contractual Data

Non-contractual data includes all acquisition documentation and other data necessary to the USTRANSCOM PMO or program. This data will be provided to CM via the CM mailbox at USTCJ6-P-CM@USTRANSCOM.MIL. Typical documents that fall into this category include, but are not limited to:

- Capability Design Document
- Initial Capabilities Documents
- Security Classification Guides
- Security Accreditation Documents
- Memorandum of Agreement

- Memorandum of Understanding
- Service Level Agreements
- Analysis of Alternatives

4.1.3 Inventory Data

The DPS CM controls the inventory data to include COTS hardware and software, and licensing information necessary to the USTRANSCOM PMO or program. This data will be provided to CM via the CM mailbox at USTCJ6-P-CM@USTRANSCOM.MIL. Typical inventory data includes, but is not limited to:

- COTS hardware listings including model and serial numbers, and suite information
- COTS software listings including versions, patches, and vendor
- Licensing information including quantity and suite information
- Hardware and COTS software maintenance information

4.2 Documentation Reviews

The USTRANSCOM PMO CM provides delivered documentation review control for DPS. The delivered documentation review process is defined in paragraph 5.12. The review times listed below D.may be modified by the PM based on size and quantity of the documentation being received. See Appendix D for the Delivered Document Points of Contact Table

Table 2 Document review dates:

Drafts	10 working days
Finals	5 working days

5 Configuration Management Process

The DPS CM process will facilitate an orderly management of system and product information and changes for such beneficial purposes as to revise capability; improve performance, reliability, or maintainability; extend life; reduce cost; reduce risk and liability; or correct defects. The DPS CM Process is shown in Figure 2 below.

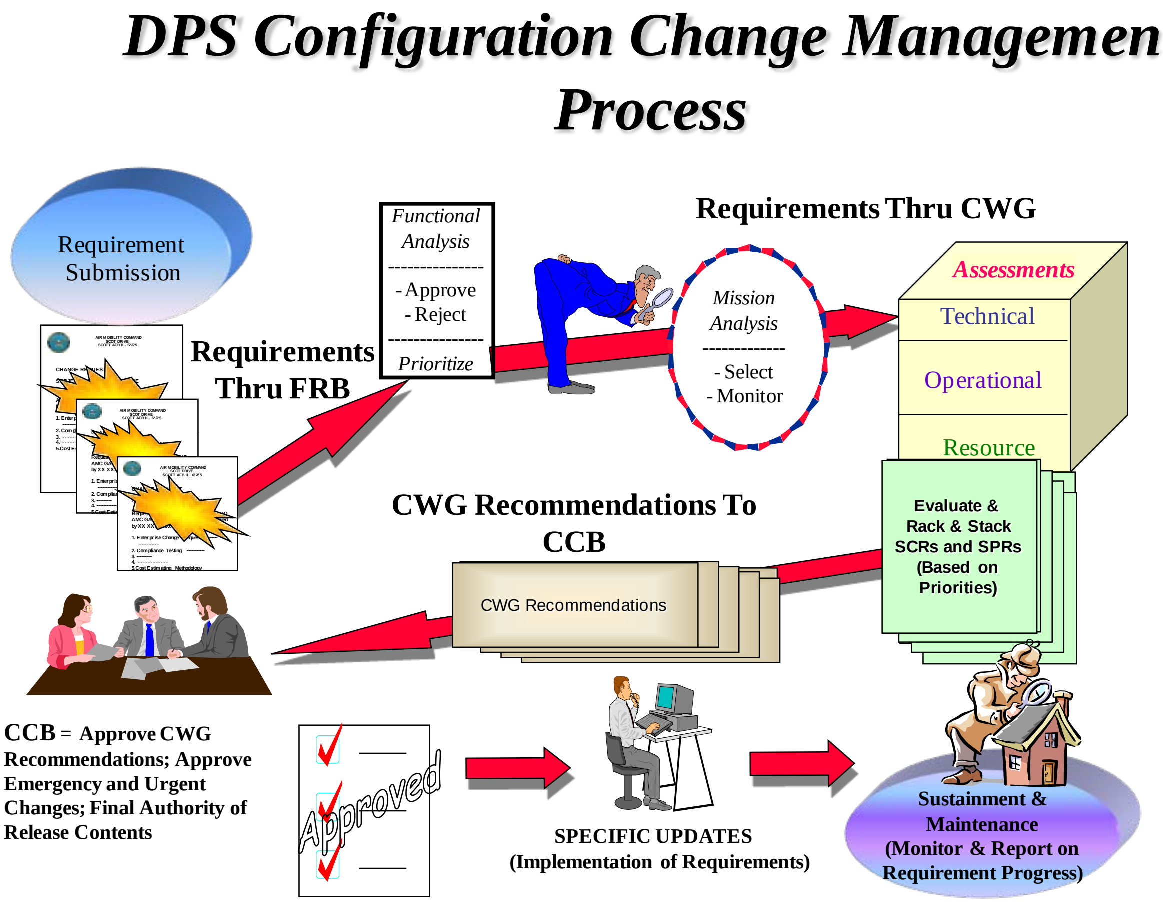
DPS Configuration Change Management Process
Requirement Submission
Requirements Thru FRB
Functional Analysis
- Approve
- Reject
Prioritize
Requirements Thru CWG
Mission Analysis
- Select
- Monitor
Assessments
Technical
Operational
Resource
Evaluate & Rack & Stack SCRs and SPRs (Based on Priorities)
CWG Recommendations To CCB
CWG Recommendations
CCB = Approve CWG Recommendations; Approve Emergency and Urgent Changes; Final Authority of Release Contents
Approved
SPECIFIC UPDATES (Implementation of Requirements)
Sustainment & Maintenance (Monitor & Report on Requirement Progress)

Figure 2 DPS configuration Change Management Process

5.1 Configuration Management Process Relationships

The DPS CM process is one aspect of the DPS overall change management process. The CM process aligns with the USTRANSCOM CM process is complemented by the development contractor's CMP. Within the JPMO, new requirements submitted via the FRB. Similarly, the CCB is only one aspect of the DPS CM process. For example, not all changes to DPS systems will be reviewed by the FRB and or CCB as specified in this CMP. However, all changes are approved by the Program Manager.

5.2 DPS Detailed Process

Configuration management activities are supported by the DPS FRB (J5/4) (as described in the RMP), a CWG and a CCB (described in the CCB Charter.) Detailed information for the DPS CWG is provided in the following paragraphs. Refer to the FRB Charter for detailed procedures for the FRB. Refer to the CCB Charter for its detailed procedures. Refer to section 5.10 for the Deliverable Documentation Review process.

5.3 Configuration Identification

Configuration identification is an evolutionary process to identify the baseline characteristics. This process identifies a baseline of physical characteristics that describe the CI and identifies the documentation to define the baseline. The first activity the configuration management process must perform is the identification and labeling of CIs that are to be placed under configuration control.

The configuration identification process ensures that all acquisition and sustainment management disciplines have common sets of documentation as the basis for developing a new system, modifying an existing component, buying a component for operational use, and providing support for the system and its components. The configuration identification process also includes identifiers that are short hand references to items and their documentation.

The Configuration Item identification activity establishes the basis for control and status accounting of a system and its change items throughout the system's lifecycle. Configuration Item identification process includes:

- Selecting change items at appropriate levels to facilitate documentation, control, and support of the items and their documentation
- Determining types of change documentation required for each CI to define its performance, functional, and physical attributes including internal and external interfaces
- Determining the appropriate change control authority for each CI
- Issuing identifiers for the CIs
- Maintaining CI change identification to facilitate effective change control of items in service
- Establishing change baselines for control of CIs

CI selection separates system components into identifiable subsets to manage, document, and control changes or further development (e.g., software, hardware items, etc.). The system engineering process produces the system architecture and the optimized functional and physical composition of the system architecture to the level necessary to specify and control item performance. Program and contract work breakdown structures (WBS) are views of the system architecture structure identifying hardware, software, services, and data against which costs are collected. CIs may be identified as WBS elements such as a SCR

Configuration items are assigned unique tracking numbers for hardware, software, documentation, and communication change items. In addition to the unique tracking number, the database will identify, as required, the organization, functional area, and military nomenclature. HWCIs will include information provided by the COTS dealer such as developer part number for each CI, serial and lot number, and description of the proposed change.

Configuration Identification includes the selection of items that are placed under the formal control of the CCB including CIs, the numbering and naming for each CI, and the determination of the type of documentation required for each CI. General categories of CIs include system components, requirements, hardware, software, and documentation.

5.3.1 Software Configuration Items

Computer Software Configuration Items (CSCIs) are assigned unique identifiers in accordance with the plan written by the contractor and approved by the Government. The contractor is responsible for recommending potential CIs to the Government. The Government makes the final selection of CIs. Software configuration items are maintained by the contractor.

All software procured under this contract with program funds and in the contractor's control will be turned over to the Government at the end of the contract.

5.3.2 Numbering Scheme for System Releases

The DPS Version Control process is an administrative system that helps the government and the developer meet contractual responsibilities. An important element of this process is the definition of key terms.

Not all requirements are the same in size and scope. Throughout the course of a development cycle, certain Software Change Requests (SCRs) are completed and rather than wait on an already scheduled Major Release, a Minor Release may be added to the release schedule.

Minor Releases are opportunities to provide upgrades and enhancements to the user. However, if a unique situation should arise, the CCB may authorize the acceleration of the Major Release date or add Minor Release dates to the schedule. Accelerations of Major Releases and additions of Minor Releases may have a severe impact on the overall DPS development schedule and therefore should only be used in the direst of circumstances. The CCB must review impacts of these actions and work with the developer to adjust requirements as needed.

Maintenance fixes and security upgrades are expected in the development of software. A Service Pack release provides a fix or update to the program, but NO new functionality is to be introduced with a Service Pack.

An emergency change request must address only one problem. If the request addresses more than one problem it will be broken up into several change requests and the priority of each change request will be reevaluated. For emergency change requests:

- CCB Configuration Manager submits the change request to the CCB Chairperson.
- The CCB Chairperson confirms the need for the emergency change request with the requester.
- If confirmed, the CCB Chairperson transmits the decision to the Configuration Manager.
- The Configuration Manager develops the change request, tasks the development team, and notifies the CCB Chairperson of the tasking. If it is not possible to perform a change and regression test the Configuration Manager should notify the CCB Chairperson immediately.
- When the change and testing have been completed the development team reports a successful test to the Configuration Manager and the CCB Chairperson. The change request package is then fully acceptance tested.
- Complete change request documentation will be included in the next scheduled FRB and CCB agendas.

An urgent change request must address only one problem. If the request addresses more than one problem it will be broken up into several change requests and the priority of each change request will be reevaluated. For urgent change requests:

- CCB Configuration Manager will submit the change request to the CCB Chairperson.
- The CCB Chairperson confirms the need for the urgent change request with the requester.
- If confirmed, the CCB Chairperson transmits the decision to the Configuration Manager.

- If an urgent change is date-driven, such a regulatory change, and the next regularly scheduled CCB will not address the change in the required timeline, the Configuration Manager will schedule an impromptu CCB within three days.
- If an urgent change is not a date-driven change, it will be developed and considered at the next regularly scheduled CCB meeting.
- Complete change request documentation will be included in the next scheduled FRB agenda.

5.3.3 Version Control Numerical Designation

The USTRANSCOM PMO uses a three-tier numbering scheme to identify system releases. This numbering scheme may also be used for individual CSCIs dependent on the tool being use by the contractor. System version numbers will be assigned by the USTRANSCOM PMO CM and approved by the PM.

The first number in the Version is the Major Release indicator (e.g., DPS Version 8). The next number is the Minor Release. Minor Releases contain Functional Enhancements as approved by the CCB. Sometimes Minor Releases are referred to as Functional Releases. Minor Releases should be scheduled by the CCB, however if they resolve an urgent priority SCR as defined in the DPS CCB Charter they can be scheduled with only CCB Chairperson approval as long as the CCB is advised at the next meeting.

The final two digits in the Version number is the designation of a Service Pack Release or Maintenance Release. These releases are used to correct functional problems with previous releases and provide maintenance or security upgrades. The CCB is advised of and approves all Service Pack Releases.

All system releases to the Government must be identified using the following as shown in tables 5 and 6:

Table 3 USTRANSCOM PMO System Version Numbering Convention

The format for the USTRANSCOM PMO Software version number is XX.YY.ZZa, where:			
XX	=	Major Release	Identifies a MAJOR change to the system as determined by the Government PM and USTRANSCOM PMO CM. A Major release will normally require reaccreditation. See discussion in 5.6
YY	=	Minor Release	Identifies a MINOR change to the system as determined by the Government PM and USTRANSCOM PMO CM. A Minor release may require reaccreditation or an Authority to Operate (ATO) determination.
ZZ	=	Maintenance Release	Identifies a MAINTENANCE change to the system as determined by the Government PM and USTRANSCOM PMO CM. A Maintenance release normally requires an ATO determination and not reaccreditation.
a	=	Emergency Releases	Identifies an Emergency Release to fix an error identified with a previously released version as determined by the Government

The format for the USTRANSCOM PMO Software version number is XX.YY.ZZa, where:			
			PM and USTRANSCOM PMO CM. An Emergency release normally requires an ATO determination and not reaccreditation.

Intermediate and/or test releases should use the approved system version number plus a fourth digit for a build number. This allows the contractor to release multiple versions of the software for testing or any other purposes deemed necessary.

All intermediate/test system releases to the Government must be identified using the following:

Table 4 USTRANSCOM PMO Intermediate System Version Numbering Convention

The format for the USTRANSCOM PMO Intermediate Software version number is XX.YY.ZZ.BN, where:			
XX	=	Major Release	Identifies a MAJOR change to the system as determined by the Government PM and USTRANSCOM PMO CM
YY	=	Minor Releases	Identifies a MINOR change to the system as determined by the Government PM and USTRANSCOM PMO CM
ZZ	=	Maintenance Releases	Identifies a MAINTENANCE change to the system as determined by the Government PM and USTRANSCOM PMO CM
BN	=	Build Number	Identifies an intermediate release to the Government for testing; this number will be incremented for each intermediate release. The final product will have this number deleted.

5.3.4 Hardware Configuration Items (HWCI)

Hardware configuration control is primarily the responsibility of the Government. The engineering branch coordinates the hardware maintenance effort, with recommendations from the contractor(s). The Government tracks the HWCI, major components, and the software. For equipment items acquired and delivered by the contractor(s), the contractor will supply inventory data to the Government. Operational equipment is maintained in an official Government account which is the responsibility of the PM and must be inventoried annually. Any changes made to the equipment at an operational site require DPS CCB approval unless it is an emergency fix. All emergency fixes must be reported to the DPS CCB within 24 hours. The information must include what was changed, updated, deleted, or replaced along with serial numbers so the Government can track changes as they occur.

All hardware procured under this contract with program funds and in the contractor’s control will be turned over to the Government at the end of the contract.

5.3.5 Documentation

The USTRANSCOM PMO CM team has established an electronic documentation library to store and maintain copies of all system documentation. The library is accessed using a database front-end to allow USTRANSCOM PMO personnel to locate a document without having to know the file structure used to store the documents. Additional documentation that needs to be placed under CM control will be emailed to CM via the CM mailbox at USTCJ6-P-CM@USTRANSCOM.MIL and will be stored in the library.

The USTRANSCOM PMO has established a document naming convention which is defined in Table 6 below. All documentation delivered to the USTRANSCOM PMO will include the system acronym, system version (if applicable), document title, document version number (change number if applicable), and status of draft or final. All e-mails to the USTRANSCOM PMO should include the system acronym in the title of the e-mail so we can easily determine which system the email is associated. See Appendix E for examples.

5.4 Configuration or Change Control

Configuration or change control is the systematic classification, evaluation, disposition and implementation of formally approved changes to a DPS configuration item and configuration documentation as identified and established by the baseline. Configuration control will regulate changes to DPS and future personal property systems from the baselines established by DPS. This section describes assigned responsibilities for each step of the configuration control process. The configuration control process provides:

- Control during each life-cycle management milestone/phases (i.e., analysis, development, design, implementation, termination of legacy system) and appropriate control over the program documentation
- Complete, accurate, and timely evaluation, assignment of priorities, and documentation of a change's impact on the configuration
- Controlled procedures for processing and implementing the changes in response to system deficiencies or mission impact

Change control is the systematic process for controlling changes to baselines and other controlled items.

Configuration Control is used to manage preparation, justification, evaluation, coordination, approval or disapproval, and implementation of proposed changes to any baseline CI and configuration documentation. Once a baseline has been established, all changes must be processed according to established configuration control procedures. Changes occur for a number of reasons, such as to insert new technology, respond to technical and operational tests and evaluations, or correct problems. The primary objectives of configuration control are to:

- Establish and maintain a systematic configuration management process
- Provide efficient processing and implementation of functional changes that maintain or enhance operational readiness, supportability, interchangeability, and interoperability
- Ensure complete, accurate, and timely changes to documentation maintained under appropriate functional control authority
- Eliminate unnecessary change proliferation

Classes of change (Class I or Class II) are defined as change requests that affect the functional or technical characteristics of a baseline. Class I changes are change requests that directly affect operation of the system; Class I changes are approved by the CCB. Class II changes are change requests that do not affect operation of the system; Class II changes are approved by the CCB Chairperson, do not require CCB approval, and are presented at the next CCB as a matter of record. The vast majority of change requests for DPS are Class I.

Examples of Class I changes:

- New or changed functional requirements (or the transfer of existing requirements to other organizations)
- Changes to configuration items, data elements, codes, and formats
- Changes in schedules or frequency of reports, statistics, update

Class II change requests (i.e., change requests are changes which have no impact on system operations). Class II change requests correct errors in a baseline or represent a minor change, which can be classified as maintenance.

Examples of Class II changes are:

- Minor hardware or software modifications or reconfiguration of equipment at the end user location
- Minor software changes such as installing security updates to software in the product baseline
- Minor changes, such as correcting misspellings, adding clarifying notes, and recompiling erroneous codes

Initial priority level is determined by the DPS Test Director. There are three different priority levels of change: Emergency, Urgent, or Routine.

<u>Emergency change request:</u> An emergency priority is a change which must be accomplished as soon as possible (ASAP). It is approved directly by the JPMO HHGS CCB Chairperson and is not required to go through the CCB. After-the-fact copies of the completed emergency change request will be distributed to each CCB member. Configuration information will be sent to the Configuration Manager for input into the appropriate baseline and will be documented.

Emergency situations require immediate corrective action by the user or operation in situations where:

- A cycle halt or abnormal termination in the production environment prohibits mission accomplishment
- Usable output critical to mission accomplishment is not produced

<u>Urgent change request:</u> An urgent priority is a change that must be accomplished expeditiously. Time constraints for implementing the change must justify its development and testing as an interim change instead of a regular change.

Urgent data-driven regulatory changes result from decisions or policy directives of an authority higher than the CCB; for example, any Service Secretary, the Department of Defense, the Congress, or the Office of Management and Budget.

Life-cycle savings through value engineering or other cost reduction efforts, so that expediting the change could decrease the cost.

<u>Routine change request:</u> A routine priority is assigned to changes when an emergency or urgent request is not applicable. Routine changes include other changes than those classified as emergency or urgent.

Once a baseline has been established, all changes must be processed according to established change control procedures. Change control must be in place for all system components and support items including hardware, software, Government Furnished Equipment (GFE), documentation, etc. Change control is currently managed by the developer's change management tool.

DPS uses a FRB, CWG, and a CCB to control changes to the system. Additional working groups may be formed on an as needed basis to forward issues and concerns to the CCB for consideration.

5.4.1 CWG Membership and Responsibilities

The DPS CWG is a team that reviews, researches and validates the DPS SCRs and SPRs in preparation for service consideration in release planning. In addition, the CWG will evaluate the level of effort, technology and system requirements specific to each change as the group prepares recommendations to the CCB for which release a change should be scheduled based on priority and resource capacity.

Areas of responsibility include, but are not limited to, the following:

- Review and validate SCR/SPR category assignment
- Remove and consolidate duplicate SCRs/SPRs
- Review of SCR form and validation of completion of business requirement at a high level
- Review of SPR and confirmation that SPR is documented thoroughly in order for JPMO and the Development Team to troubleshoot the issue
- Conduct impact assessments on requested changes
- Provide cost, schedule and technical recommendations to the CCB
- Escalate issues and change activities to the CCB

The CWG is formed under the authority of the CCB and meets as necessary. The CWG will review all issues and items brought to them for consideration. These items include unresolved service requests (SR), proposed releases, Engineering Change Proposals (ECPs), requests for deviations, etc. Other items may be brought as deemed necessary and appropriate for the CWG.

Membership in the CWG includes all DPS contractor and Government personnel deemed necessary by the CWG Chair (DPS Government Lead). This includes USTRANSCOM PMO DPS testers, CM, engineers, functional representatives, helpdesk members, developer CM, development contractors, etc.

General membership responsibilities include ensuring the agenda and issues are reviewed prior to the meeting so members can discuss the items for the function they are representing.

5.4.2 CWG Process

The CWG determines the validity of all items and issues brought before it and prepares each item for CCB presentation if required.

The CWG reviews all items brought to it by the helpdesk, USTRANSCOM PMO support, development contractor, functional, and the USTRANSCOM PMO CM. This will include helpdesk tickets not resolved by the helpdesk, change requests, operational issues, etc. The CWG validates requirements from the FRB and issues from the SRC, then groups like items into specific releases. Once releases and issues are approved by the CWG they will be presented to the DPS CCB for formal disposition.

Findings, defects or Software Problem Reports (SPRs) identified during formal test evolutions will be linked to the appropriate CI and given a classification and priority. SPRs will be tracked to completion by the JPMO Test Director and Configuration Manager and approved by the CCB or reported to the CCB as required. In the case where it is determined that a SPR can only be resolved via a SCR, the SCR process outlined in this document will be followed.

Problems identified by users and recorded via a trouble ticket that are not resolved within the appropriate amount of time will be evaluated by the CCB Configuration Manager to determine if a SCR is necessary. Once a determination has been made, the SCR will be linked to the appropriate CIs and given a classification and priority. At this time the remainder of the SCR process outlined in this document will be followed.

5.4.3 CCB Membership, Responsibilities and Processes

Refer to the DPS CCB Charter for details of CCB membership and responsibilities.

5.4.4 Baselines

Baseline Development and sustainment efforts for DPS will contain three separate baselines.

- The Functional Baseline (FBL): The Functional Baseline describes the system or top-level requirements. This includes the system/top-level functional, performance, interoperability and interface requirements and the verifications required to demonstrate the achievement of those requirements.
- Allocated Baseline (ABL): The Allocated Baselines draw on the functions, identifying the individual components that are needed to perform the functions. The Allocated Baselines govern the development of releases.
- The Product Baseline (PBL): The Product Baseline is a more detailed extension of the previous baselines. It provides a level of detail and documentation necessary to produce and support an operational release.

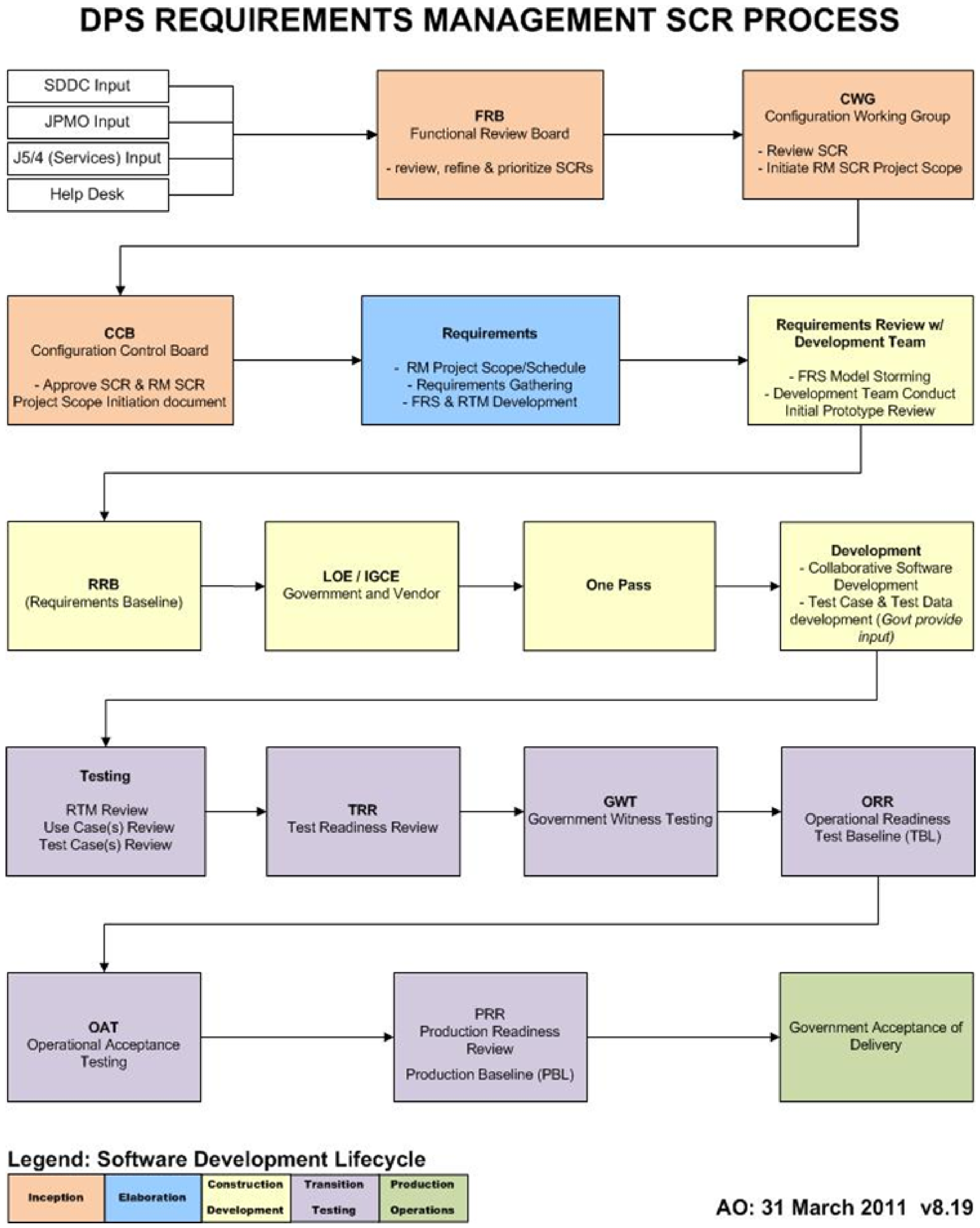
DPS REQUIREMENTS MANAGEMENT SCR PROCESS
SDDC Input
JPMO Input
J5/4 (Services) Input
Help Desk
FRB
Functional Review Board
- review, refine & prioritize SCRs
CWG
Configuration Working Group
- Review SCR
- Initiate RM SCR Project Scope
CCB
Configuration Control Board
- Approve SCR & RM SCR Project Scope Initiation document
Requirements
- RM Project Scope/Schedule
- Requirements Gathering
- FRS & RTM Development
Requirements Review w/ Development Team
- FRS Model Storming
- Development Team Conduct Initial Prototype Review
RRB
(Requirements Baseline)
LOE / IGCE
Government and Vendor
One Pass
Development
- Collaborative Software Development
- Test Case & Test Data development (Govt provide input)
Testing
RTM Review
Use Case(s) Review
Test Case(s) Review
TRR
Test Readiness Review
GWT
Government Witness Testing
ORR
Operational Readiness
Test Baseline (TBL)
OAT
Operational Acceptance Testing
PRR
Production Readiness Review
Production Baseline (PBL)
Government Acceptance of Delivery
Legend: Software Development Lifecycle
Inception
Elaboration
Construction
Development
Transition
Testing
Production
Operations
AO: 31 March 2011 v8.19

Figure 3 DPS Enhancement Process showing baselines.

5.4.5 Systems Engineering Lifecycle

DPS will employ baselines throughout the program life cycle. These baselines, when documented and approved, constitute the foundation for controlling changes to DPS. Configuration identification establishes a baseline only when formally designated and fixed at a specific time as a reference point for change control.

The DPS program will adhere to the processes and procedures identified in the DPS System Engineering Plan (SEP), when available, for lifecycle requirements.

5.5 Configuration Status Accounting (CSA)

CSA is the recording and reporting of information needed to effectively manage the status of CM controlled items and CM activities. CSA produces a list of the approved configuration items, the status of proposed changes to the system, and the implementation status of approved changes.

CSA tracks the current approved configuration baselines, operational units, and changes placed under configuration control. CSA also monitors all related tasks resulting from such changes and the status of problems/change requests affecting the entity. The function's structure and methods are dictated by the program's needs, the volume of change activity, and imposed constraints. The Configuration Manager selects specific data elements, records and report formats and the record keeping methods. These choices will be made during the life cycle of DPS with the advice and concurrence of the CCB.

The Configuration Manager will prepare and maintain records and reports of the configuration status of each CI. These records and reports will be kept in the CM Library for the lifecycle of the project and will include the current version and related changes of each CI, a record of change to the CI since being placed under configuration control, and the status reports affecting the CIs.

CSA records and the resultant reports will exist in numerous formats and in varying detail. The CCB maintains records and reports to track distribution of changes and authorized versions and their location. CSA is initiated when the Functional/Requirements and Design/Development baselines are established and expanded, as baselines develop into configuration identifications. The CCB library and/or information system used by the CCB to perform CSA will, at a minimum, be capable of identifying software vendor name, software name, version, software origin, role, date acquired, maintenance expiration, serial number/license key, physical location of software and/or license material, and current maintenance information such as expiration date and current recurring cost of maintenance, SCRs and SPRs represent changes to the system and their status updates are contained in SharePoint / Program Tracker.

The development contractor is responsible for keeping status accounting records and providing reports to the CWG as stated in their Performance Work Statement (PWS).

5.6 Configuration Audits

Configuration audits validate the accuracy of the configuration documents and configuration items. Audits will be used to verify compliance with specifications and related documents. The acquisition process is evolutionary to allow for incremental delivery of capabilities that ultimately provide the total desired system capability and environment to satisfy emerging requirements. The product baseline for each delivery is established after an audit of the delivered system. The audits covered under this document are defined below:

The CCB will support and conduct configuration audits as outlined below.

- A Configuration Audit (CA) formally validates that the DPS development has been completed satisfactorily and that a CI has achieved the performance and functional characteristics specified in the functional or development configuration identification.
- The CCB Chairperson or Configuration Manager, with approval from the CCB, will conduct the CA.

The CA is conducted on a CI to ensure that the:

- CI's technical documentation accurately reflects the CI's functional and physical characteristics
- Software's technical documentation accurately and adequately describes the software
- Software is supportable and maintainable

The CA may be conducted on a progressive basis (when so determined) throughout the CI's development and culminates with acceptance testing of the software and a final review of all CA discrepancies. The CA also establishes that acceptance testing of the product CIs is valid. To do this, the CA compares the acceptance test procedure and test results with the product CI performance requirements, as specified in the development specifications. The CA and approval of the product CI establish the product baseline.

The Functional Configuration Audit (FCA) ensures that as-built products have satisfied their specified and approved requirements while the Physical Configuration Audit (PCA) ensures that as-built products are developed as specified in their design artifacts. Completion of these audits establishes the PBL.

The Government reserves the right to participate in any development audits and/or review results of audits upon request.

5.7 DPS Change Processes

Changes or change proposals to the DPS systems are called defects or enhancements. The DPS CCB decision on any change proposal is documented on the DPS CCB - System Change Request Form (Appendix B) that becomes the formal record of the decision. The System Change Request Form contains each Service's/Organization concurrence or nonoccurrence with the CCB decision, and the approval/disapproval date. Pertinent comments from the members should be attached to the Change Request Form.

The determination of which SCRs ultimately end up in a DPS version release is the responsibility of the DPS CCB. This group is responsible for determining what functional capabilities and program upgrades are released in designated versions.

Some of these requirements are simple and do not take significant resources to implement. Some however, may span several years. The CCB works to develop a release schedule which takes into account all the resource considerations and provides the development contractor with a clear expectation for system development. Minor Releases and Service Packs can be made throughout the year on an as needed basis. When possible, these activities should be scheduled by the DPS CCB during one of their regularly scheduled meetings. Minor Releases and Service Packs deemed to have urgency can be developed and released out-of-cycle as needed to meet special situations. These types of releases should be kept to a minimum, and need to be briefed at the next CCB meeting. The CCB would then need to study and determine if the “out-of-cycle” releases had an impact to the existing version release schedule.

5.7.1 DPS Defect Process

Defects are imperfections or anomalies that impair the use of the product and may be found during testing or by the user. Defects found by the user start out as SRs. Defects found during testing are SPRs.

The members of the CWG will review each defect enhancement and SR that cannot be resolved by the SRC team for validity and accuracy. If the request is valid, the members will assign a priority, severity (for defects only), determine if the enhancement should be classified as a minor or major enhancement, and estimate the effort to correct. This request will then be added to the task list to be worked or be added to the defect or enhancement pool for consideration at a later date.

a. Priorities are subjective and may change and should be assigned based on the items that are to be fixed first. All change requests are prioritized.

b. Severities are determined by how a defect affects the system. They objective based on the following guidelines and seldom change. Only SPRs, TPRs, or PRs are given severities.

Table 5 Defect Severity Descriptions

Severity	Description
1	System or major component of the system is inoperable
2	System or major component of the system is inaccurate and there is no work around to the problem
3	System or major component of the system is inaccurate but there is a work around; need to publish the work around
4	Inconvenience to the user
5	Minor inconvenience to the user or aesthetic issue
6	COTS issue – cannot be resolved until the COTS is updated

The DPS program development contractor is responsible for the formal tracking of all defects associated with the operational DPS system. Defects are normally received through the DPS SRC for calls which cannot be closed at the SRC level (Tier 1). All defects will be entered into the change control tool, reviewed and dispositioned by the CWG. The CWG will determine severity, priority, determine if a workaround is available, and a release recommendation if appropriate. Periodically the CWG will review outstanding defects and enhancements and group appropriate items into release candidates for submission to the DPS CCB for review and disposition.

Defects may also be identified during government test events. Defects identified during government test events will have unique identifier assigned. This identifier allows the USTRANSCOM PMO to perform metrics as necessary to determine the number of defects being found during government testing and number of defects being found by operational users.

After completion of each government test event, the CWG will compile the test results to include any outstanding Test Problem Reports (TPRs) and present the information to the DPS CCB with recommendation for an ORR or PRR. The DPS CCB determines if any particular release is acceptable for operational use. See paragraph 5.7 for more information on the Test and Release process.

Any TPRs identified as enhancements at the CWG will be handled as other enhancements, see paragraph 5.7.2 below.

Figure 2 below depicts the Defect process.

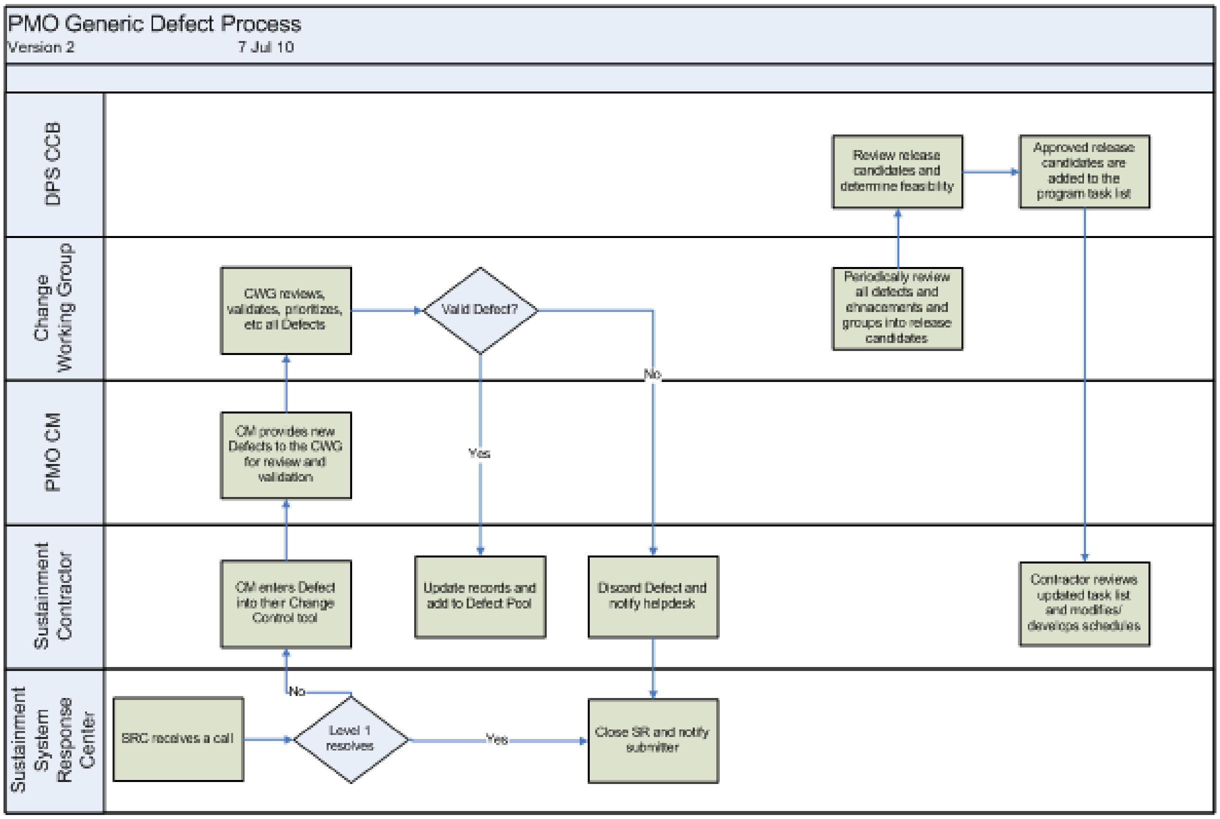
PMO Generic Defect Process
Version 2
7 Jul 10
DPS CCB
Change Working Group
PMO CM
Sustainment Contractor
Sustainment System Response Center
Review release candidates and determine feasibility
Approved release candidates are added to the program task list
CWG reviews, validates, prioritizes, etc all Defects
Valid Defect?
Periodically review all defects and ehnacements and groups into release candidates
No
CM provides new Defects to the CWG for review and validation
Yes
CM enters Defect into their Change Control tool
Update records and add to Defect Pool
Discard Defect and notify helpdesk
Contractor reviews updated task list and modifies/ develops schedules
No
SRC receives a call
Level 1 resolves
Yes
Close SR and notify submitter

Figure 4 DPS Defect Process

5.7.2 DPS Enhancement Process

Enhancements are changes to the system that include additional capability which the system is not currently designed to perform. These would include the addition of an interface, performing additional calculations, adding screens or reports, etc. Enhancements may or may not affect the security posture of the system. To assist the PM in identifying which changes may affect the security posture, enhancements are further categorized as minor or major enhancements. Minor enhancements are those enhancements that the USTRANSCOM PMO believes will not affect the security posture of the system. They may include building additional screens or reports with data already available in the database, changing data element sizes or properties, etc. Major enhancements are assumed to affect the security posture and would require a re-accomplished ATO. This will aid in estimating the lead time required for a security determination when the USTRANSCOM PMO defines the content of a release and builds its release schedule.

SCRs that affect a DPS baseline and/or a CI will be evaluated and processed in accordance with the DPS RMP and CCB Charter. The HHGS Configuration Manager will create a consolidated presentation package in support of the proposed SCRs for each CCB meeting. However, it is the responsibility of the change proponent to research and provide required documentation in support of a change for use by the CCB. Individual members of the CCB will study, evaluate, and discuss proposed changes and other agenda items before the CCB is convened. Factors that the CCB should consider when evaluating potential changes include design, performance, schedules, reliability, security, cost, interfaces, operational effectiveness, safety, human factors, logistics support, and training.

Refer to the DPS RMP for more detailed enhancement procedures. Also refer to the CCB Charter for CCB process details.

Updates to COTS products present a special challenge. Most updates to these products have periodic patches provided by the vendor, updates driven by security issues (normally associated with an Information Assurance Vulnerability Alert (IAVA), Information Assurance Vulnerability Bulletin (IAVB), Information Assurance Vulnerability Technical Advisories (IAVTA), or other vulnerability management issue), or new versions of the COTS product. Periodic patches can normally be added to a scheduled minor or maintenance release, time permitting, and should not affect the security posture of the system. If the update needs to be implemented prior to the next scheduled release, the USTRANSCOM PMO can decide to do an Emergency Release or implement as a Site Configuration Change. Security and IAVA updates change the security posture, but the change is positive since the update is correcting a security issue identified with the product. A new version of a COTS product will normally be considered a possible change in security posture, but will only modify the minor release digit.

The DPS program development contractor is responsible for the formal tracking of all enhancements associated with the operational DPS system as stated in their PWS. Enhancements may be received through the DPS SRC for calls which cannot be closed at the SRC level, but can also be sent directly to the USTRANSCOM PMO CM or be provided by the Functional proponent. All enhancements will be entered into the change control tool, reviewed and dispositioned by the CWG. The CWG will make recommendations to the DPS CCB as to the enhancement’s priority, whether the enhancement is classified as a major or minor enhancement, and a release recommendation if appropriate. Periodically, the CWG will review outstanding defects and enhancements and group appropriate items into release candidates for DPS CCB review and disposition.

See Figure 3 for the DPS Enhancement Process flow.

5.8 DPS Test and Release Process

Refer to the DPS Test and Evaluation Master Plan for detailed test procedures. Figure 4 below shows the DPS Release Process.

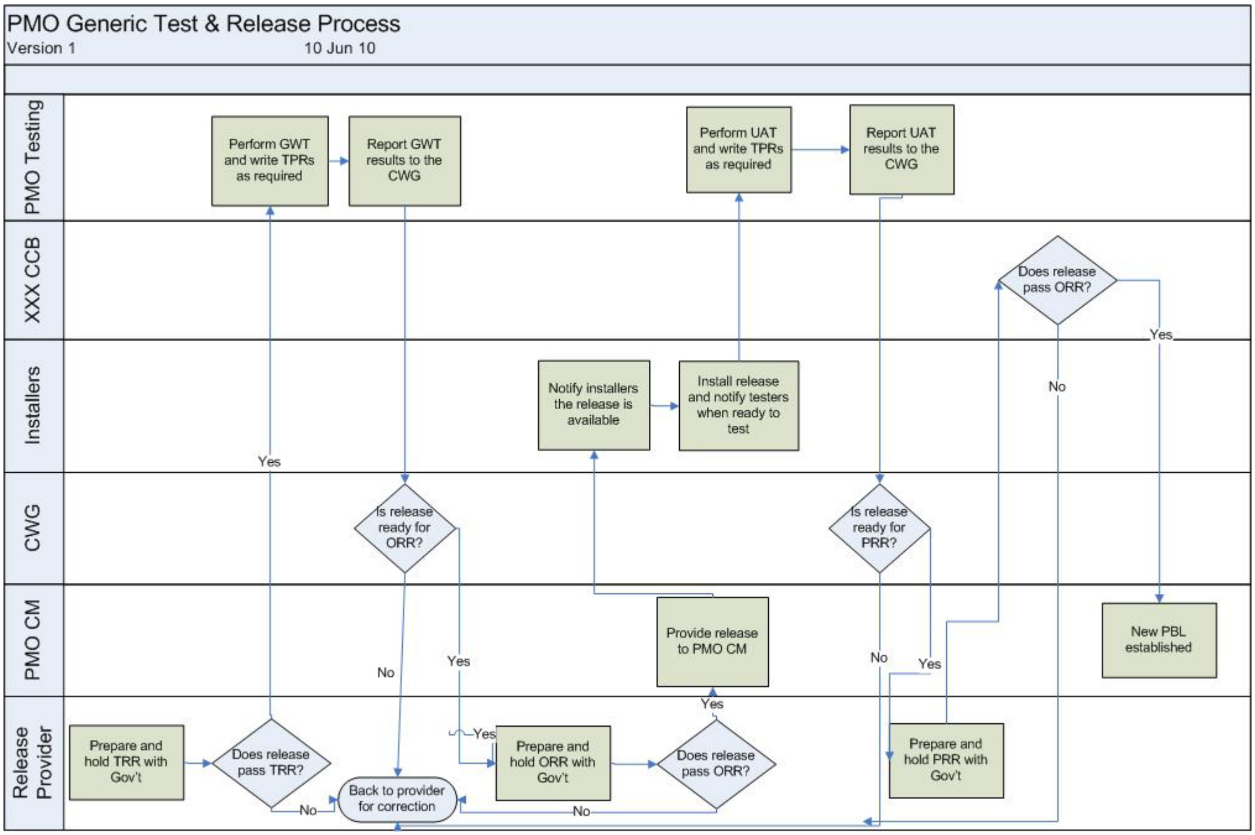
PMO Generic Test & Release Process
Version 1
10 Jun 10
PMO Testing
XXX CCB
Installers
CWG
PMO CM
Release Provider
Perform GWT and write TPRs as required
Report GWT results to the CWG
Perform UAT and write TPRs as required
Report UAT results to the CWG
Does release pass ORR?
Yes
No
Notify installers the release is available
Install release and notify testers when ready to test
Yes
Is release ready for ORR?
Is release ready for PRR?
No
Yes
Provide release to PMO CM
No
Yes
New PBL established
Yes
Yes
Prepare and hold TRR with Gov't
Does release pass TRR?
No
Back to provider for correction
Prepare and hold ORR with Gov't
Does release pass ORR?
No
Prepare and hold PRR with Gov't

Figure 5 DPS Release Process

5.9 Major and Minor Release Process

In order to meet the scheduled version release dates the government and the development contractor must understand the version release process. Key documents must be developed and published. Key activities, such as scheduling for the release to be installed in the test environment first and the independent validation and verification (IV&V) testing, Operational Assessment Testing and GOSC approval (for all major releases) need to be completed in order to ensure version release dates are met. The Schedule is a key management tool for the DPS program. The Development Contractor, Functional Representative, and the PM should stay aware of the schedule. The CCB should be briefed on the status of the project schedule. Forecasted slippages in the schedule should be addressed by the CCB. If appropriate, reprioritization of requirements should be reviewed in order to get the schedule back on track. If necessary the CCB Chair (PM) has the authority to request additional resources to meet any schedule problem.

5.10 DPS Document Review Process

The USTRANSCOM PMO CM receives all documentation from the contractor directly into the USTCJ6-P-CM@USTRANSCOM.MIL organizational mailbox. CM logs the documentation into the library database, develops a document review form for the specific document, and forwards the comment form to the document POC and required reviewers with required suspense dates. The document POCs may forward the information to other reviewers they think need to review the document. The document POC consolidates the comments into a single comment form and returns them to CM by the suspense date. CM reviews the comment form for completeness and provides the formal Government comments to the contractor's POC.

The diagram below graphically depicts the document review process. See section 4.2 for the list of document POCs and associated review times.

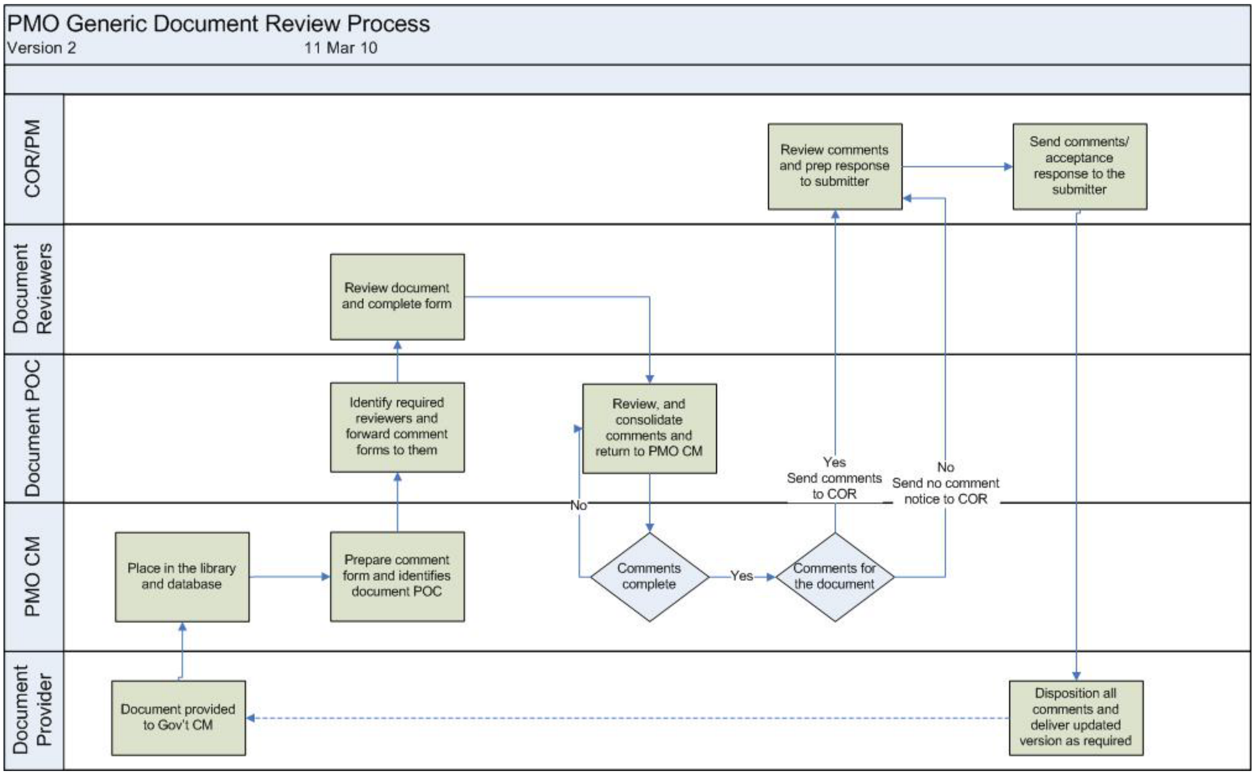
PMO Generic Document Review Process
Version 2
11 Mar 10
COR/PM
Document Reviewers
Document POC
PMO CM
Document Provider
Review comments and prep response to submitter
Send comments/ acceptance response to the submitter
Review document and complete form
Identify required reviewers and forward comment forms to them
Review, and consolidate comments and return to PMO CM
Yes Send comments to COR
No Send no comment notice to COR
No
Place in the library and database
Prepare comment form and identifies document POC
Comments complete
Yes
Comments for the document
Document provided to Gov't CM
Disposition all comments and deliver updated version as required

Figure 6 DPS Document Review Process

6 Appendix A. Acronyms

2DMSL	Two-dimensional Military Shipping Labels
ABL	Allocated Baseline
ASAP	As Soon As Possible
ATO	Authority to Operate
BVS	Best Value Scoring
CA	Configuration Audit
CCB	Configuration Control Board
CDR	Critical Design Review
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
COTS	Commercial Off-the-Shelf
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
CWBS	Contractor Work Breakdown Structure
CWG	Change Working Group
DM	Data Management
DOD	Department of Defense
DP3	Defense Personal Property System
DPS	Defense Personal Property System
ECP	Engineering Change Proposal
FBL	Functional Baseline
FCA	Functional Configuration Audit
FRB	Functional Requirements Board
FS	Functional Specification
GFE	Government Furnished Equipment
GIG	Global Information Grid
GOTS	Government Off-The-Shelf
HHGS	Household Goods Systems
HWCI	Hardware Configuration Items
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVTA	Information Assurance Vulnerability Technical Advisories
IMS	Integrated Master Schedule
IVR	Interactive Voice Recognition
IV&V	Independent Validation and Verification
J2EE	Java 2 Enterprise Edition
JPMO	Joint Program Management Office
LCM	Life-Cycle Management
LMS	Learning Management System
MIL-HDBK	Military Handbook
ORR	Operational Readiness Review
PBL	Product Baseline
PCA	Physical Configuration Audit

PM	Program Manager
PMO	Program Management Office
POAM	Plan of Action and Milestones
POC	Point of Contact
PPCIG	Personal Property Consignment Instruction Guide
PRR	Production Readiness Review
PWS	Performance Work Statement
RMP	Requirements Management Plan
SCR	Software Change Request
SDDC	Surface Deployment and Distribution Command
SEP	System Engineering Plan
SPR	Software Problem Report
SR	Service Request
SRC	System Response Center
SRR	System Requirements Review
TOMP	Task Order Management Plan
TOPS	Transportation Operational Personal Property Standard
TPPS	Third Party Payment System
TPR	Test Problem Report
TSP	Transportation Service Providers
USTRANSCOM	United States Transportation Command
WBS	Work Breakdown Structure

7 Appendix B. DPS CCB Voting Form

DPS CCB – VOTING FORM

*** *ITEMS 1-7 TO BE FILLED IN BY THE CCB CHAIRPERSON OR CONFIGURATION MANAGER* ***

1. SCR NUMBER: __________________________

2. STATUS: { } APPROVED { } CONDITIONALLY APPROVED
{ } DEFERRED APPROVED { } DISAPPROVED
{ } UNRESOLVED, FORWARDED TO USTRANSCOM
STATUS DATE: ________________ RELEASE (IF APPLICABLE): ______________

3. CONFIGURATION LEVEL: { } HARDWARE { } SOFTWARE { } OTHER: _________________

4. SYSTEM: { } DPS { } OTHER: ____

5. CHANGE CLASSIFICATION: { } CLASS I { } CLASS II

6. EVALUATION REQUIREMENTS:
A. CCB: { } YES { } NO { } N/A
B. TECHNICAL PANEL: { } YES { } NO { } N/A
C. FUNCTIONAL PANEL: { } YES { } NO { } N/A
D. SECURITY PANEL: { } YES { } NO { } N/A
E. OTHER: ___________________ { } YES { } NO { } N/A

7. FUNDING PROFILE & COST: { } FUNDED { } UNFUNDED { } OTHER: __________________

*** *ITEMS 8-12 TO BE FILLED IN BY REQUESTER* ***

8. PRIORITY: { } ROUTINE { } URGENT { } EMERGENCY

9. DATE CHANGE REQUEST SUBMITTED: ___________________

10. REQUESTER (NAME/ORGANIZATION/PHONE NUMBER/EMAIL):
____

11. SUMMARY OF CHANGE REQUEST:
A. NARRATIVE/DESCRIPTION OF PROBLEM/CHANGE: ___________________________________
B. RECOMMENDED SOLUTION(S) OR ALTERNATIVES (IF ANY): __________________________
C. NEED FOR CHANGE & BENEFITS: ____

12. WHAT ARE KNOWN IMPACTS (OTHER SYSTEMS AFFECTED OR SCHEDULE CHANGES):
____

*** *CCB SIGNATURES & APPROVAL/DISAPPROVAL* ***
(ATTACH SHEET WITH REASON IF MEMBER DISAPPROVES OF CHANGE REQUEST)

USA REP ______________________ { } APPROVAL { } DISAPPROVAL DATE _________
USN REP ______________________ { } APPROVAL { } DISAPPROVAL DATE _________
USMC REP ______________________ { } APPROVAL { } DISAPPROVAL DATE _________
USAF REP ______________________ { } APPROVAL { } DISAPPROVAL DATE _________
USCG REP ______________________ { } APPROVAL { } DISAPPROVAL DATE _________
USTRANSCOM REP__________________{ } APPROVAL { } DISAPPROVAL DATE _________

13. SIGNATURES: _____________________________ _____________________________
CCB Chairperson Configuration Manager

8 Appendix C. CCB Meeting Minutes Form

DPS CCB MEETING/MINUTES FORMAT

THE FOLLOWING WILL BE INCLUDED AT A MINIMUM IN CCB MEETING MINUTES

1. CCB MEETING ATTENDEES: NAME/ORGANIZATION/LOCATION

A. ____

B. ____

C. ____

2. ENCLOSURES:

3. MEETING SUMMARY:

4. APPROVAL OF MINUTES & DOCUMENTS FROM THE LAST CCB MEETING:

A. DOCUMENT ________________ { } APPROVED { } DISAPPROVED

B. DOCUMENT ________________ { } APPROVED { } DISAPPROVED

C. DOCUMENT ________________ { } APPROVED { } DISAPPROVED

D. DOCUMENT ________________ { } APPROVED { } DISAPPROVED

5. STATUS OF CCB CHANGE REQUESTS:

A. SCR #: ____________________

B. NARRATIVE: ____________________________

C. PRIORITY: ____________________________

D. STATUS: ____________________________

E. FUNDING: ____________________________

F. COMMENTS: ____________________________

6. BASELINE (CONFIGURATION ITEMS) SUMMARY OF CHANGES:

A. ____

B. ____

C. ____

7. OPEN CCB ACTION ITEMS:

8. UNRESOLVED ISSUES:

9. NEW ISSUES:

10. PROPOSED DATE OF NEXT CCB MEETING

11. CCB CHAIRPERSON SIGNATURE: _____________________ DATE: ________

9 Appendix D. Delivered Document Points of Contact Table

Document Type	POC	Required Reviewers
Design: Software / Architecture / Database	Ralph Meacham	Virginia Menz Ken Whitaker Carl Mattison
Security/Information Assurance	Ralph Meacham	Virginia Menz Tom Payne Carl Mattison Chris Boerner
System Performance Metrics	Ralph Meacham	Ralph Meacham Virginia Menz
Interfaces	Betty Soto	Ralph Meacham Virginia Menz
Test (Test Cases)	Roni McDaniels	Hank Gawlik Doug Beauvais
Functional (Use Cases and RTMs)	Roland Amos	Stan Quinn Roni McDaniels Virginia Menz Stephen Ratermann
Training	Roland Amos	Stan Quinn Mike Crimens Mary Lewis
Operations	Kenneth Whitaker	Amie Davis Stephanie McPherson
System Response Center (SRC)	Kenneth Whitaker	Roland Amos Stan Quinn
Task Order Management Plan (TOMP) Integrated Master Schedule (IMS) Contractor Work Breakdown Structure (CWBS)	Stefanie McPherson	Alan Lee Ralph Meacham Kenneth Whitaker Roland Amos Tim Knapp Virginia Menz

10 Appendix E. Naming Conventions

Table 6 USTRANSCOM PMO Naming Convention Examples for Documentation

System Acronym	System Version if Applicable	Document Title	Rev or Ver	Draft Final	File Ext
DPS		DPS CCB Meeting Minutes and Slides	Mar 11	Final	.docx
DPS	DPS 1.4.07	Requirements Traceability Matrix (RTM)		Final	..xls

Table 7 Naming Convention Examples with Change Identification

System Acronym	System Version if applicable	Document Title	Rev Ver	Change Number	Draft Final	File Ext
DPA		IBR	Ver 03	.3	Final	..ppt
DPS		Rate Filing Users Guide – Govt Edition	Ver 5	.2	Draft	.doc

Table 8 Naming Convention Examples for Attachments

System Acronym	System Version if applicable	Document Title	(Attachment Number) Attachment Name	Rev Ver	Change Number	Draft Final	File Ext
DPS		DPS Database Design Document (DBDD)	Appendix A - ECP PDM Table Metadata	May 08		Final	..xls
DPS		DPS Economics Analysis (EA)	Attachment E		.	Final	..ppt
DPS		DPS Initial Capabilities Document (ICD)	Appendix C Acronym List	Ver 6		Final	.doc