Net-Enabled Command Capability

INCREMENT 1 SYSTEM DEVELOPMENT AND DEMONSTRATION (SDD) PHASE

CONFIGURATION MANAGEMENT PLAN

27 July 2007

Version 1.0

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502
In Collaboration with the Joint Forces Command and NECC Component Program Manager's for Navy, Air Force, Army, Marine Corps, and DISA.

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (27 July 2007). Other requests for this document shall be referred to the NECC Program Management Office.

DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

APPROVAL PAGE

Approved by: Laura D. Knight Date: 27 July 07

LAURA D. KNIGHT
Program Manager,
Joint Program Management Office (JPMO),
Net-Enabled Command Capability (NECC)

EXECUTIVE SUMMARY

This Net-Enabled Command Capability (NECC) System Development and Demonstration (SDD) Phase Configuration Management Plan (CMP) defines the strategies needed to accomplish the configuration activities and configuration management processes for the Joint Program Management Office (JPMO) and supplies direction to the Component Program Management Offices (CPMOs) required for:

1. Configuration Identification (CI)
2. Configuration Control
3. Configuration Status Accounting (CSA)
4. Configuration Audits and Reviews

REVISION HISTORY

Version Number	Reviewer / Org	Changes	Version Date	Date Entered	Name of Person Entering Change
0.0.1	JMH/SAIC	Initial Draft	June 2007	June 2007	Jacqueline Harkins
0.0.2	DLB/SPEC	Formatted document according to NECC/DISA standards	27 June 2007	27 June 07	Dustan Brown
0.0.3	PJS/NECC	Various	28 June	28 June 07	Paul Stoskus
0.0.4	IGJ/BIT (NECC Documentation Support	Reformatted and edited the document; reset figures to display better; fixed headers and footers; generated a new TOC; changed version number and updated Revision History page to reflect changes made.	25 July 2007	25 Jul 07	Issa Jones
0.0.5	DLB/SPEC	Final editing and formatting for signature	26 July 2007	26 July 07	Dustan Brown
1.0	DLB/SPEC	Final formatting	27 July 2007	27 July 07	Dustan Brown

This Configuration Management Plan (CMP) is subject to annual review and update by the Joint Program Management Office (JPMO). Review and update will also take place when any of the following situations occur:

1. Changes in scope or management processes that necessitate a change in configuration constructs.
2. Identification of process improvement activities after approval of the CMP.
3. Identification of activities that are determined to be critical after approval of the CMP.
4. Changes in tools and techniques.

Changes to the CMP are reflected on this page. Each revised plan is subject to the NECC program process for document review and approval before becoming final. When approved, a new version of the CMP is issued and all members of the team and affected groups are informed as to the changes made.

TABLE OF CONTENTS

APPROVAL PAGE ..... **II**

EXECUTIVE SUMMARY ..... **III**

REVISION HISTORY ..... **IV**

1 INTRODUCTION **1**

1.1 PRODUCT DESCRIPTION 1
1.2 OBJECTIVE 2
1.3 SCOPE 2
1.4 REFERENCED DOCUMENTS 2
1.5 CMP STRUCTURE 3

2 CONFIGURATION MANAGEMENT ORGANIZATION **3**

2.1 GENERAL 3
2.1.1 JPMO Roles and Responsibilities *4*
2.1.2 CPMO Roles and Responsibilities *4*
2.1.3 Joint Forces Command *5*

3 CONFIGURATION CONTROL **5**

3.1 BASELINE MANAGEMENT 5
3.2 CONFIGURATION CONTROL ROLES AND RESPONSIBILITIES 6
3.2.1 Configuration Management Board *7*
3.2.2 NECC Configuration Control Board *7*
3.2.3 Critical Configuration Area CCB *8*
3.2.4 Critical Configuration Item CCB *9*
3.2.5 Engineering Review Board *9*
3.2.6 Local CCB *9*
3.3 NECC CHANGE CONTROL PROCESS 10
3.3.1 NECC Change Request Process *10*
3.3.2 Change Request Documentation and Tracking *13*

4 CONFIGURATION IDENTIFICATION AND SELECTION **14**

4.1 NECC CONFIGURATION BASELINE 14
4.2 NECC CRITICAL CONFIGURATION ITEM IDENTIFICATION 14
4.2.1 CCA/CCI Approval Process *15*
4.2.2 CCA/CCI Registration Process *17*
4.2.3 CCA/CCI Selection Process *17*
4.3 INTERFACE MANAGEMENT AND CONTROL 18

5 CONFIGURATION MANAGEMENT ACTIVITIES **18**

5.1 NECC BASELINE DEFINITIONS 20
5.1.1 Increment Requirements Baseline *20*
5.1.2 Functional Baseline *20*
5.1.3 Allocated Baseline *21*
5.1.4 Product Baseline *21*
5.1.5 Deployed Baseline *21*
5.2 VERSION CONTROL 21
5.3 CONFIGURATION MANAGEMENT AUDITS 22
5.3.1 Physical Configuration Audit *22*
5.3.2 Functional Configuration Audit *22*
5.3.3 Release Audit *23*
5.3.4 Library Audit *23*
5.3.5 Process Audits *23*

5.3.6 Configuration Management Reviews *23*
5.4 CONFIGURATION STATUS ACCOUNTING 24
5.4.1 Reporting *24*
5.4.2 Metrics *25*
6 TRAINING 25
7 TOOLS 26
APPENDIX A – ACRONYMS 21
APPENDIX B – GLOSSARY OF TERMS 21
APPENDIX C – CONFIGURATION ITEMS SELECTION PROCESS EVALUATION CHECKLIST 21
APPENDIX – D NECC CRITICAL CONFIGURATION ITEM PROPOSAL 23
APPENDIX E – NECC CHANGE REQUEST FORM 24

LIST OF FIGURES

Figure 1: NECC Configuration Management Framework 7
Figure 2: NECC Configuration Control Board Organization 8
Figure 3: CCA Change Request Process 11
Figure 4: CCI Change Request Process 11
Figure 5: NECC CCA Selection Process 16
Figure 6: NECC CCI Selection Process 17
Figure 7: FDCE Stages 19

1 INTRODUCTION

1.1 Product Description

Net-Enabled Command Capability (NECC) creates software Capability Modules integrated into a Service Oriented Architecture (SOA) accessible through the Global Information Grid (GIG). The applications and databases in the NECC architecture are in accordance with Department of Defense (DoD) Net-Centric Data Strategy, and are supported by GIG Enterprise Services (GES) and Net-Centric Enterprise Services (NCES) enabling shared access to Service/Agency/Joint-provided services (data sources and applications).

NECC provides a highly flexible Command and Control (C2) architecture, and systems that integrate all aspects of national power to include not only the Defense Services and Agencies, but also State, Commerce, Homeland Security and other Departments, non-governmental agencies, and international coalition partners' militaries and agencies. NECC allows C2 of the full range of military forces and other agencies' capabilities, when and where required, achieving unified effort and commanding dominance. NECC C2 systems are effective during deliberate and crisis action planning and execution as Warfighters engage in the Force Projection Cycle. Capability Modules provide a Joint system for developing and updating time-phased force and deployment data and unit movement requirements. NECC provides the capability to continuously access, review, and update current intelligence and tactical information over a global Command, Control, Communications, Computers, and Intelligence (C4I) infrastructure that can support Joint and coalition missions. An advantage of NECC is that it provides access to common services, databases, imagery, and an open architecture to reduce the Joint decision cycle. It provides systems supporting Joint and multi-national force interoperability. NECC maximizes the use of Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) software and leverages industry standards.

NECC Increment 1 focus is the mission space from National Military Command System (NMCS) through Service/Functional Components. Increment 1 emphasizes Joint Forces Command (JFC) operations throughout the Joint Warfighting environment, keyed to capability needs in Situational Awareness and Joint operations planning, Force Projection and Force Readiness Mission Capabilities Packages (MCPs), and selected related capabilities from the other MCPs. Future increments expand to address the full NECC mission space.

NECC enables better information visibility and accessibility through infrastructure services. Understandability and consistency of authoritative data is gained through adherence to universal and common C2 data frameworks. The family of data models supports rapid search, discovery, and retrieval capabilities with reduced needs for translation and mediation.

NECC reach-back capabilities exploit global expertise and information Centers of Excellence (CoE). Deploying fewer in-theater forces also reduces force protection and sustainment needs, while enhancing overall force agility.

The NECC program is designated as an acquisition streamlining pilot program chartered to develop revised processes and products that enable a faster, more effective milestone review, and rapid capability fielding. One of the primary advantages of the NECC program is the ability to transition existing Command and Control Capabilities (C2C), while concurrently developing and fielding new or enhanced capabilities, quickly and under the direction of a common Joint

Program Management Office (JPMO). This approach affords the DoD the ability to select and rapidly implement "best-of-breed" solutions for the full spectrum of Joint C2 needs.

NECC is not building a "system"; instead, it is rapidly developing and fielding individual units of functionality called Capability Modules.

The NECC System Development and Demonstration (SDD) Phase Configuration Management Plan (CMP) provides top-level direction for incorporating configuration management practices into the NECC program JPMO and, in turn, guides configuration management implementation by NECC Component Program Management Offices (CPMOs). In addition, it describes the application of configuration management to this program and provides guidelines for implementing processes supporting this function during the SDD phase.

1.2 Objective

This CMP provides formal configuration management policies and procedures for controlling requirements, development, production, and maintenance of the NECC Technical Baseline in the SDD phase.

The objectives of the CMP are to:

- Provide the depth of control required to control the NECC Critical Configuration Items (CCIs)
- Provide a common NECC Technical Baseline reference configuration for all items to be controlled over the lifecycle phases of NECC
- Provide unity and clarification for governing bodies who review and approve NECC baselines, resources, and development
- Provide a common nomenclature to help resource and technical managers verify that product items and configurations meet source requirements
- Focus development and modification of NECC services on DoD mission areas and mission service priorities
- Ensure NECC requirements traceability and NECC product accountability.

1.3 Scope

This document describes the NECC CMP activities to be performed, and assigned responsibilities required, to support the JPMO and CPMO activities including, but not limited to, staff, tools, and computer facilities. It applies to artifacts and Capability Modules developed and maintained by the materiel providers. It supports the SDD phase of NECC to include the operational support for the Deployed Baselines. The SDD phase addresses the lifecycle of the capability increments.

1.4 Referenced Documents

The following documents are used as the foundation for creating this JPMO level CMP:

1. Defense Information Systems Agency (DISA) NECC Technology Development (TD) Phase Configuration Management Plan, Ver 1.0, June 30, 2006

2. DISA NECC Technology Development Phase Change Control Procedures, Ver 1.0.1, 29 June 2007
3. NECC Technology Development Phase Configuration Management Board and Change Control Board Charter, Ver 1.1, January 25, 2007
4. DISA NECC Critical Configuration Areas/Items (CCA/Is), Ver 1.0, January 11, 2007
5. MIL-STD 973, Configuration Management, AMSC No. D6728, Historical Document, April 17, 1992.
6. MIL-HDBK-61B, Military Handbook, Configuration Management Guidance, 10 September 10, 2002.
7. NECC Concept for Rapid Provisioning of C2 Capabilities onto the GIG dated March 27, 2006.
8. Joint Command and Control (JC2) Capabilities Development Document (CDD)
9. NECC Systems Engineering Plan (SEP), Increment 1 Milestone B, Ver 0.6, 14 May 2007
10. DRAFT NECC Developer's Handbook, Ver 0.7

1.5 CMP Structure

The CMP sections are organized as follows:

Section 1. Introduction: Describes Objective and Scope of the CMP.

Section 2. Configuration Management Organization: Describes the configuration management organization.

Section 3. Configuration Control: Describes the configuration control board responsibility and associated activities for the program.

Section 4. Configuration Identification and Selection: Describes how CCIs are selected and maintained.

Section 5. Configuration Management Activities: Describes the configuration management activities the NECC program.

Section 6. Training: Describes the training of the configuration management tools and processes.

Section 7. Tools: Describes the use of tools to aide in the control of the NECC CCIs.

2 CONFIGURATION MANAGEMENT ORGANIZATION

2.1 General

The NECC JPMO and the NECC CPMOs together form a Joint Configuration Management structure with appropriate involvement by US Joint Forces Command (USJFCOM), the requirements manager. The NECC JPMO functions as a "system prime and system integrator" of increment requirements, systems engineering, integration, and increment-level performance responsibilities. The CPMOs function as materiel developers for individual capabilities that

meet increment requirements and are responsible for integrating Capability Modules into their respective operational facilities/platforms.

2.1.1 JPMO Roles and Responsibilities

The JPMO is responsible for articulating program objectives and status to the NECC Communities of Interest (COI) as well as to the Joint Program Executive Office (JPEO) C2C.

The JPMO is responsible for defining the NECC Critical Configuration Areas (CCAs) and their associated CCIs as well as an increment's Capability Modules. It is also responsible for developing a Technical Baseline (Increment Requirement, Functional, Allocated, and Product Baselines) and for the configuration management and control of that baseline.

The primary JPMO configuration management responsibilities are:

a. **Establishing the overarching program configuration management**. In this capacity, the JPMO is responsible for developing and implementing configuration management policies, procedures, and governance structure that span the NECC Technical Baseline, to include the Requirements, Functional, Allocated, and Product Baselines. These will include artifacts such as Service Performance Specifications (SPSs), Service Level Agreements (SLA), and Capability Module work packages.

b. **Shaping policy for the CPMO Materiel Providers**. The CPMOs, in their role as Materiel Providers, will be responsible for implementing configuration management policies and procedures that support the lifecycle of the NECC Services that they provide. These include artifacts such as software and hardware. While the JPMO will not dictate how this will be accomplished, it is responsible for providing a minimum set of guidelines that will support the NECC goals.

JPMO CMP establishes a centrally located configuration management repository which enables easy reuse of resources.

2.1.2 CPMO Roles and Responsibilities

As the NECC materiel developers, CPMOs support the JPMO in achieving an increment's required capabilities. The CPMOs are responsible for providing materiel solutions for CMs as defined by the NECC Systems Engineering Plan (SEP) approved by the JPEO C2C, and executed by Work Packages. The CPMOs use their Services' contracting authority and organization to select industry partners who will develop, deliver, and sustain the capabilities required to meet NECC's requirements.

The NECC CPMO's organizations include the major component C2 system commands and agencies as well as other capability providers. These materiel providers will participate by developing, maturing, operating, and sustaining enterprise-operated Capability Modules and Capability Packages. A Capability Module is a collection of one or more services that provide an operationally useful capability that has been matured, developed, and certified. A Capability Package is a specific implementation of a Capability Module that has been compiled to run and operate in a specified computing environment.

The primary CPMOs configuration management responsibilities are:

a. **Maintaining baselines.** The CPMOs are responsible for maintaining the Capability Module's internal baselines to include performing configuration management at the CM level and participating in NECC's overarching configuration management efforts.

b. **Maintaining governance.** The CPMOs will establish and manage a Local Configuration Control Board (CCB) and Local Engineering Review Board (ERB) as well as participate in NECC CCB and the ERB.

Configuration Management supports these material providers in maintaining, tracking, and providing status accounting of the configured environments and of the documents and other Configuration Items (CIs) that are part of the operational and support environment.

2.1.3 Joint Forces Command

As the NECC requirements manager, JFCOM participates in the NECC CCB. It assists in identifying requirements affected and in analyzing the potential impact of issues.

3 CONFIGURATION CONTROL

Configuration control is the establishment of orderly and effective procedures for processing all changes to affected NECC CCIs and baseline configuration documentation. Configuration control is required to ensure systematic submission, coordination, evaluation, selection, and release of approved changes to the established NECC Baseline. Change requests to the NECC Technical Baseline, CCA/CCIs, can be initiated by NECC users, developers, test, and evaluation teams; NECC engineering activities; Help Desk process; or as a result of the Capabilities Provisioning Activities (CPAS) activities. Configuration control shall be established and implemented throughout the NECC lifecycle to ensure that only properly evaluated and approved changes are incorporated and that NECC compliance and change accountability is maintained.

This element of configuration management identifies the groups participating in the processes, provides for baseline control, and promotes interface control. Once the CCIs are established, baseline management is achieved through the application of the formal change process. For the NECC evolution, configuration control will facilitate the integration and transition of existing applications, and the sharing of the NECC infrastructure and enabling services. Configuration control encompasses the formal change process that enables conflict resolution, interface management, and program optimization.

3.1 Baseline Management

CCI selection sets the foundation for implementing the formal change processes necessary to maintain a current NECC baseline. The NECC baseline serves as a point of departure from which change is managed and subsequently measured. If necessary, the baseline may be redefined at any point in the evolution of NECC. Once defined, changes to the NECC baseline must be formally approved and documented. The CCIs approved by the NECC Configuration Management Board (CMB) form the baseline for configuration management and the formal departure point for control of future changes.

3.2 Configuration Control Roles and Responsibilities

The JPMO Configuration Management organization, described in the following paragraphs, is responsible for maintaining configuration control over the CCI developmental configurations and baselines, and for processing changes to those CCIs. This is accomplished by administering the processes of version control, change control, reporting, and auditing. The Configuration Management organization implements the processes described within this plan to ensure that products developed are correct, consistent, complete, and compliant with governing policies.

The NECC CMB is the governing body that sets configuration management objectives and priorities, and oversees CCI development and deployment activities. The NECC CCB is the primary means of establishing and maintaining the integrity of the products of the NECC throughout the program's lifecycle.

The scope of the NECC program is very large and complex and will evolve over time. Therefore, the JPMO established a tiered framework to reduce complexity through consolidation of CCIs into categories called CCAs; and, to assist in identifying and controlling the configuration baseline at the program level. (For a list of CCAs and their respective CCIs, refer to the *Net-Enabled Command Capabilities (NECC) Program Critical Configuration Areas/Items (CCA/Is)* document named in Section 1.4 of this document.) The CCAs and CCIs will be managed through their respective CCBs. These CCBs will be responsible for reporting back to and submitting issues to the NECC CCB where those issues are either out of their scope, charter, or ability to solve.

CCIs are defined as those configuration items that represent initiatives, functions, processes, and data within the NECC program, and require more focus and management review. CCAs are a logical grouping of CCIs that have common functionality, share areas of focus, or have other common attributes. Figure 1 graphically depicts this framework using a subset of the NECC CCA for illustration.

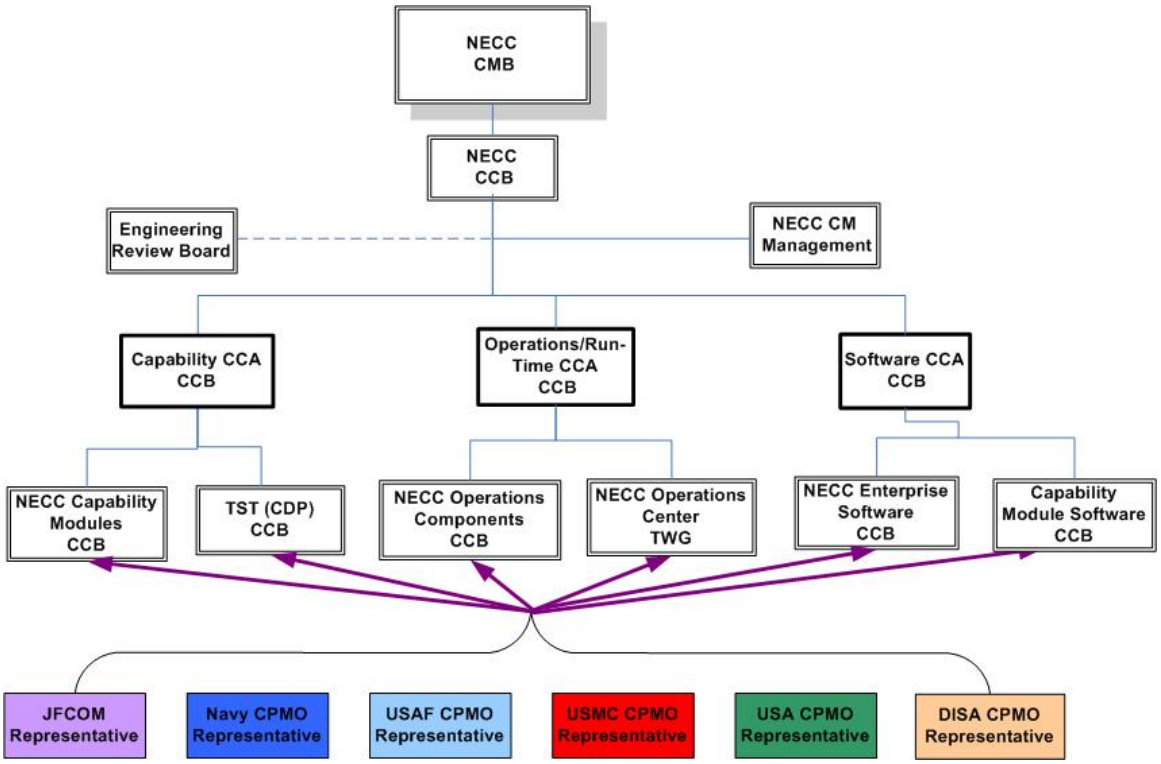

Figure 1: NECC Configuration Management Framework

3.2.1 Configuration Management Board

The NECC CMB is the configuration management governing body and the senior forum for adjudicating issues referred to it by the CCB concerning development, content, and scheduling of NECC Capability Module baseline releases. As the most senior program configuration control authority, the CMB typically only reviews Change Requests (CRs) forwarded by the NECC CCB for decision that are beyond the developers' NECC scope or funding negotiated through a SLA. The CMB will refer those that exceed pre-established thresholds to the JPEO C2C for decision.

The CMB functions primarily to resolves issues referred by the CCB. Representatives from the JPMO and each CPMO are members of this body and provide operational insight into the development of the NECC baseline.

3.2.2 NECC Configuration Control Board

The NECC CCB will establish and approve the Technical Baseline, maintain and manage formal configuration control over established baselines, ensure change requests are sufficiently defined, review and assess change requests for scope and impact, dispose of change requests, and review approved and incorporated changes to baselines. The CCB is the responsible authority for approval of recommended changes to all Capability Modules.

CCA's will be established by the CCB and will be focused to allow the distribution of the configuration management responsibilities to subordinate groups given configuration management responsibility for functionally related CCIs. For example, a Software CCA might include CCIs such as Enterprise Software, Capability Module Software, and Client Software.

The exact scope of a CCA shall be determined by the CMB at the time of creation but with recommendations provided by the NECC CCB.

The NECC CCB uses an ERB to conduct a technical review and assessment of certain change requests before determining their disposition. The ERB will elicit help from and coordinate with the appropriate Subject Matter Experts (SME) as appropriate.

Proposed changes deemed beyond the scope of the NCCB or requiring significant fiscal commitments are forwarded to the CMB for approval/disapproval. The CMB will refer those that exceed pre-established thresholds to the JPEO C2C for decision.

Representatives from the JPMO and each CPMO are members of this body and provide operational insight into the development of the NECC baseline. The CCB coordinates with the CMB in conducting its duties.

The NECC CCB membership includes representatives from the JPMO, USJFCOM, and each CPMO as depicted in Figure 2.

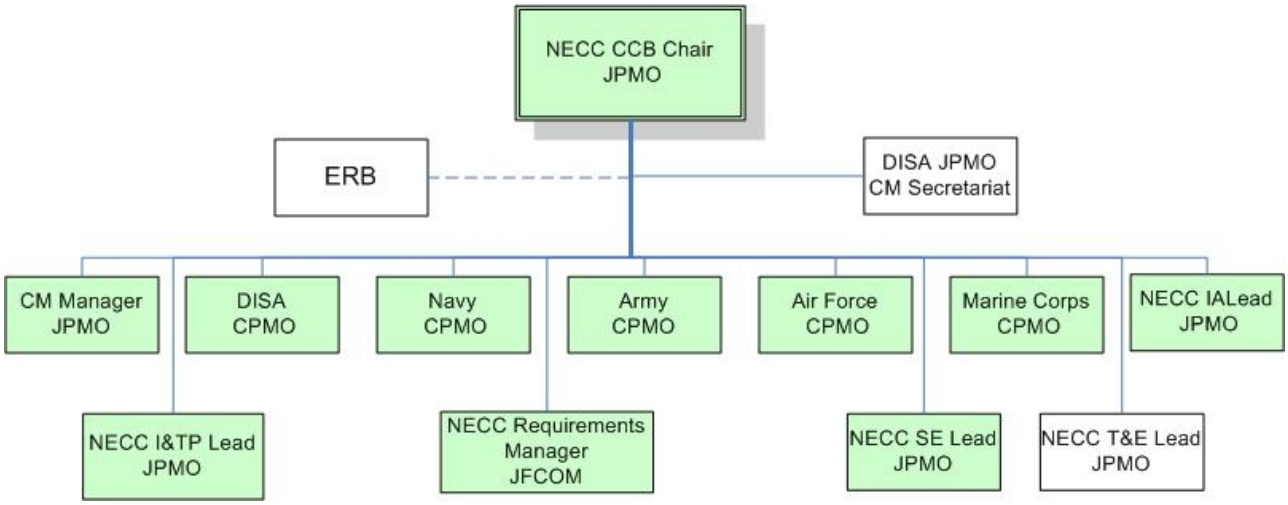

Figure 2: NECC Configuration Control Board Organization

3.2.3 Critical Configuration Area CCB

CCA CCBs serve as technical managers for the CCIs assigned to them and advise the NECC CCB on technical issues associated with any CCI under their purview. The primary responsibilities of the CCA CCBs will include the following:

a. Managing a baselined set of CCIs under its purview

b. Providing continuity and traceability of those CCIs under its purview

c. Providing the specific boundary and scope charters for the individual CCBs

d. Providing an adjudication and coordination process for the creation of Joint solutions.

CCA CCB membership includes the following:

a. Chair: NECC CCA Recognized Technical Expert

b. Administrative Region Coordinators, where applicable

c. Agency Technical Representatives (e.g., JPMO, CPMOs, JFCOM, Test and Evaluation (T&E) Lead, etc.)

d. Others as deemed necessary by the JPMO.

3.2.4 Critical Configuration Item CCB

The CCI CCBs may provide CCI specific technical inputs to the CCA CCBs or may advise on technical issues associated with other CCIs to the CCA CCBs and/or the NECC CCB. The primary responsibilities of the CCI CCBs will include the following:

a. Managing the baselined set of CCI requirements

b. Providing traceability between requirements and the current baseline

c. Providing NECC CRs against current capabilities in response to CCI CCB chairman's direction.

CCI CCB membership includes the following:

a. Chair: NECC CCI Recognized Technical Expert

b. Administrative Region Coordinators, where applicable

c. Agency Technical Representatives (e.g., JPMO, CPMOs, JFCOM, T&E Lead, etc.)

d. Others as deemed necessary by the JPMO

3.2.5 Engineering Review Board

At the direction of the NECC CCB, the ERB conducts an analysis of proposed CRs to identify critical configuration items affected by the changes and works with the appropriate CPMO to determine the costs, impacts, and benefits associated with proposed CR.

ERB members speak for the JPMO and CPMO they represent and are expected to articulate the technical position of that CPMO in meeting discussions and decisions. These members serve as technical advisors to the NECC CCB.

The ERB is a voting body and decisions are made based on consensus. Each member participating in the ERB will have one vote for approval/disapproval of recommended technical assessment of changes brought before the Board.

3.2.6 Local CCB

The Local CCB shall have cognizance over the individual Capability Modules' internal baselines. The Local CCB is responsible for assessing proposed changes and known problems reported against the materiel solution (Capability Module), adjudicating change requests, and maintaining configuration control of the Capability Modules assigned to them as the materiel provider. The Local CCB is responsible for approving code changes that affect version numbers at the third or fourth digit. Changes that affect the first and second digit of a Capability Module's version or changes that may affect the interface must be approved at the NECC CCB. This Local CCB will provide detailed information and recommendations on issues that must be elevated to the NECC CCB level.

3.3 NECC Change Control Process

The purpose of the Change Control Process is to initiate, monitor, and facilitate implementation changes that cross systems or processes between functional communities. These changes across systems or processes are referred to as NECC CRs. The goals of the Change Control Process are to:

a. Effectively manage, implement, and track the NECC CRs
b. Provide a method for the initiator to ascertain the status of a CR
c. Ensure feedback to the appropriate authority for model updates (e.g., data, network)
d. Identify duplicate activities across systems and functions
e. Identify common data elements across systems
f. Identify and establish new CCIs
g. Ensure communication among CR initiators, coordinators, and reviewers
h. Monitor the status of a CR and feedback to end-users
i. Provide open communications to raise issues associated with CRs
j. Ensure a streamlined method for conflict resolution
k. Provide a method to measure the success of the process
l. Enable continuous process improvement based on the measures or metrics
m. Identify training requirements
n. Facilitate operational assessment of the change in capability.

3.3.1 NECC Change Request Process

An overview of CCA change control document flow from request to resolution of change is shown in Figure 3, and the same for a CCI change control process is shown in Figure 4. Each major function follows NECC configuration management procedures and uses standard CM documents and formats that must be produced and exchanged with other major functions.

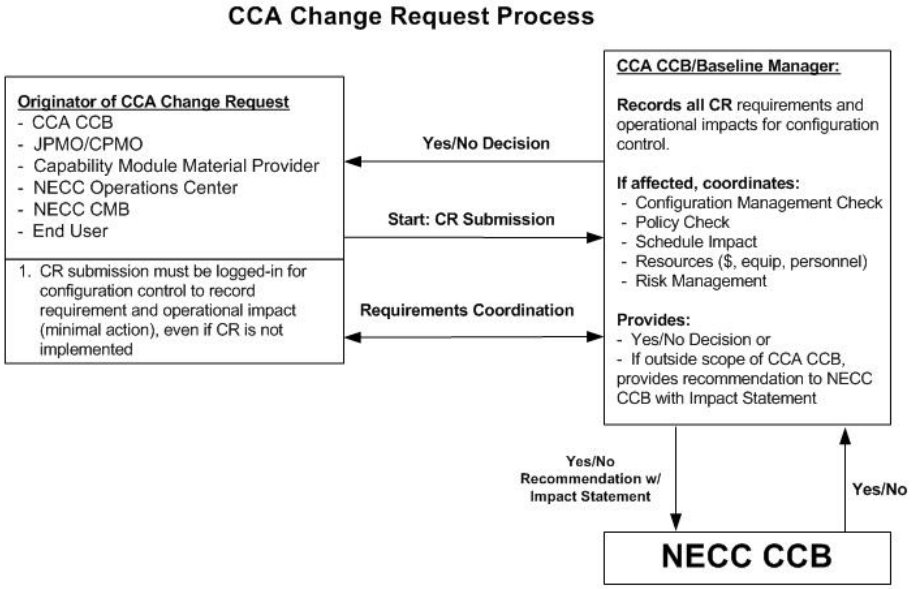

Figure 3: CCA Change Request Process

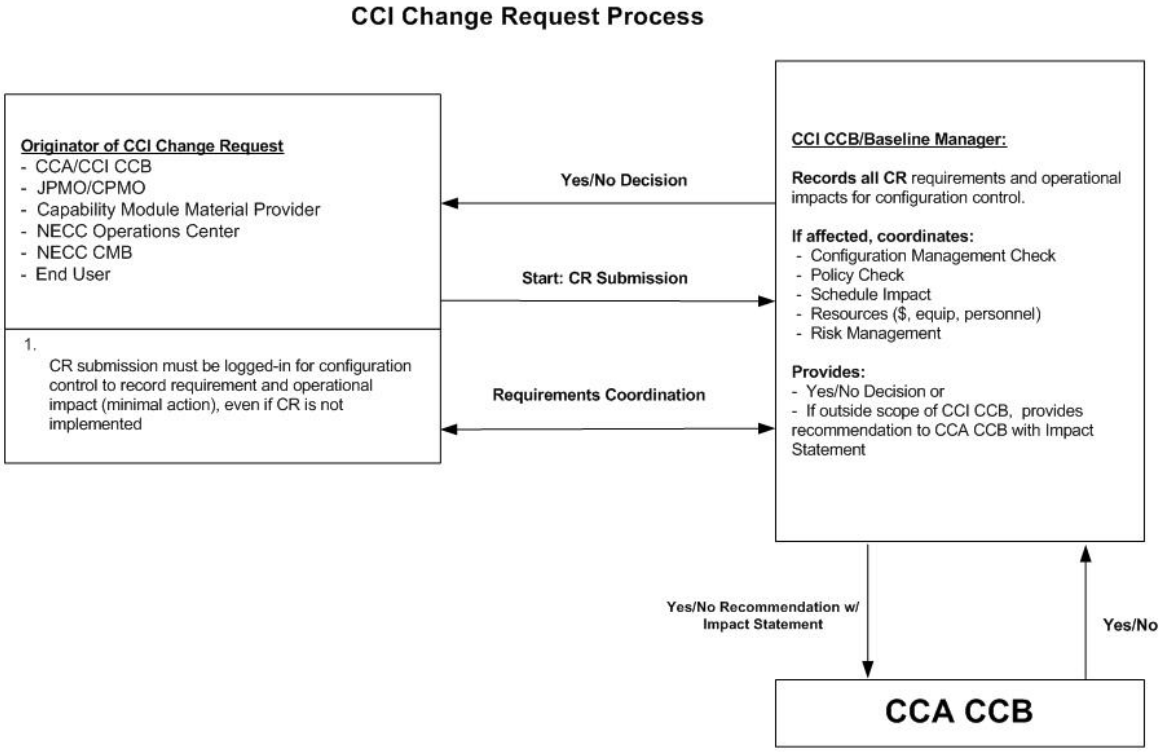

Figure 4: CCI Change Request Process

3.3.1.1 Change Request Initiation

The change process begins when a CR is received by CM. CRs can be originated by anyone involved in the NECC program. Typically a CR will be the result of a Problem Report (PR) generation through the NECC Help Desk. Once a PR is received at the Tier 1 Help Desk, and it is determined to be irresolvable at this level the PR is elevated to the Tier 2 Help Deck. Tier 2 level personnel will review the PR and determine if the reported problem requires a CR. If this determination is made, s/he will create a CR. If at the Tier 2 level a determination cannot be made, it will be elevated to the Tier 3 Help Desk at which point a CR will be completed by a SME.

Additionally, CRs may be submitted by materiel developers, or testers. They may also be generated as a result of the CPAS activities.

The CCB Secretariats will query the CR database weekly to access all CRs under their CCB's purview. All CRs must be submitted using the format of the CR sample in Appendix E.

Once a CR is received, the CCB will:

a. Ensure that the CR is not duplicative of another CR already in the system

b. Ensure that the information in the CR is complete and complies with established policies and procedures

c. Provide a recommended CR priority

d. Contact the sponsoring organization and request they submit additional detail if needed prior to the CCB meeting

e. Coordinate the schedule for a CCB review.

3.3.1.2 CCA/CCI CCB Review of Change Request

The CCB review will include the following tasks:

a. Approve the recommended CCA or CCI prioritization or re-prioritize CRs.

b. Identify CR resource requirements and determine if resources are available to implement the CR.

c. Determine if CR implementation will impact other CCIs and coordinate the requirements with other CCI CCB chairs

d. Approve, disapprove, or defer CRs that are within the authority of the CCI CCB. CRs outside of that authority will be graduated to the CCA CCB

e. Document CR activities

f. Provide CR recommendations with impact statement to the NECC CCB for review.

3.3.1.3 NECC CCB Review of Change Requests

The NCCB review will consist of the following tasks:

a. Assess proposed CRs

b. Validate resource requirements

c. Validate impact to other CCIs

d. At the direction of the Chairperson, CRs that are deemed technical in nature are forwarded to the ERB for technical assessment

e. Approve, disapprove, or defer CRs that are within the authority of the NECC CCB. CRs outside of that authority will be graduated to the NECC CMB

f. Provide recommendations with impact statement to the NECC CMB for review and approval/disapproval, if required

g. Provide documented feedback of recommendations and NECC CMB decisions to the CCI CCB and the originator.

3.3.1.4 ERB Review of Change Requests

When a CR is referred to the ERB for assessment, the ERB:

a. Provides technical assessment of CR with its proposed disposition to include cost, schedule, performance implications, and/or impact analysis summaries

b. Determines if the CR affects a change to a CDP and forwards to USJFCOM for Joint Combat Capability Development (JCCD) requirements analysis, then reports this action back to the NECC CCB

c. Ensures that all NECC Requirements Identification Database (NRiD) ERB entries are acted upon/closed out within the NRiD in a timely manner

d. Apprises the NECC CCB of significant changes to the NECC Technical Baseline.

3.3.1.5 NECC CMB Review of Change Requests

The NECC CMB review will consist of the following tasks:

- Review CRs that have been referred by the NECC CCB, which are beyond the developers' NECC scope or operating budget or the funding negotiated through an SLA.

  a. Refer those recommendations that exceed pre-established thresholds to the JPEO C2C for decision

  b. Document the decisions for each CR under their purview

  c. Provide documented decisions to the NECC CCB.

3.3.2 Change Request Documentation and Tracking

The CCB CR decision and all supporting documentation must be made available to the appropriate NECC organizations. The appropriate CCB Secretariat will update the status of the CR to include CCB decision and supporting documentation in the CR database.

This section will further address the incorporation of approved CRs into the affected baseline, prior to Milestone (MS)-C as the program's processes mature and as we gain experience managing the complexities of configuration management in this web-enabled, SOA-based program environment.

4 CONFIGURATION IDENTIFICATION AND SELECTION

Configuration Identification and Selection is the process of defining and documenting the technical description of system components under configuration control throughout their lifecycle. Baseline documents identifying the requirements, functional, allocated, product, and deployed physical and performance characteristics of NECC capabilities plus approved changes to the baseline constitute the current Configuration Identification and Selection process.

NECC Configuration Identification and Selection process shall support controlled development and maintenance of NECC capabilities throughout their respective lifecycles. Baseline configuration documentation shall be established and maintained consistent with capability development for each spiral level. Baseline documentation shall clearly identify the Service's functional capabilities and performance requirements of NECC capabilities to ensure orderly transition from one major functionality increment to the next in system requirements identification, engineering, design, and development processes.

4.1 NECC Configuration Baseline

NECC CCI selection is the primary activity within the element of configuration identification. Effective configuration identification is a pre-requisite for the other configuration management activities (configuration control, status accounting, and auditing), which all use the products of configuration identification. Selection of CCIs establishes the NECC configuration baseline. The collective identification of CCIs creates the foundation for baseline establishment and management as well as document and model control. Once CCIs have been identified, they are subject to the formal change process within the functional element of configuration control. With the baseline established, a formal departure point for control of future changes is founded. If necessary, a baseline may be redefined at any point in the continuous process improvement effort.

It is anticipated that not all designated CCIs will require a formal configuration baseline. Procedures for managing CCIs without a formal configuration baseline will be addressed in updates to this document as change control procedures are implemented, program configuration management experience accumulates, and lessons learned become available.

4.2 NECC Critical Configuration Item Identification

As stated previously, CCIs are defined as those configuration items which represent initiatives, functions, processes, and data within the NECC program that impact or are shared among multiple organizations across the DoD. The NECC CCI document (referred to Referenced Documents) provides the list of currently approved CCIs.

Initially, a CCI proposed CI will be assigned to a CCA for further analysis. The CCA will determine if the CI meets the criteria to become a CCI. A CCB will be established for each CCI with a configuration baseline and assigned the authority to oversee the selection and management of that CCI. If the CCA CCB rejects a CCI, but determines that the item may warrant the establishment of a Technical Working Group (TWG), then the CCA CCB will forward that recommendation to JPMO SE for consideration. Additions or changes to the NECC CCIs will follow the Change Control Process outlined in Section 3.3 of this document.

Going forward, CCIs may be added to the baseline set of CCIs during the evolution of the NECC. The addition of CCIs or modification of existing CCIs will follow the process discussed in Section 3.3 of this document. It is anticipated that the majority of these CCIs will come from the JPMO/CPMOs via the Milestone Review Process. The NECC CCB will support the NECC CMB in establishing the necessary interface to the Milestone Review Process.

Adoption and retirement of NECC CCAs and CCIs will be recommended by the NECC CCB and approved by the NECC CMB. As long as their configuration management practices comply with the NECC CMP guidance and implementing procedures found here and in similar program documents, material providers will have discretion to establish the configuration management framework for their configuration items that best fit their needs. Changes to the baseline will be implemented and documented and will undergo continuous improvements via an iterative management process.

The configuration identification process at the NECC level includes:

a. Selecting CCIs within the NECC to facilitate the documentation, control, and support of the items

b. Determining the types of configuration documentation required for each CCI to define its performance, functional, and physical attributes including internal and external interfaces

c. Determining the appropriate configuration control authority for each configuration document consistent with logistic support planning for the associated CCI

d. Issuing identifiers for the CCIs and the configuration documentation

e. Maintaining the configuration identification of CCIs to facilitate effective logistics support of items in service

f. Releasing configuration documentation

g. Establishing configuration baselines for the configuration control of CCIs

4.2.1 CCA/CCI Approval Process

As stated previously, one of the goals of the Configuration Management process is to identify and establish new NECC CCAs and CCIs. A high level process has been established for the registration, selection, and subsequent approval/disapproval of CCAs and CCIs. Figure 5 provides a high level view of the CCA Selection process.

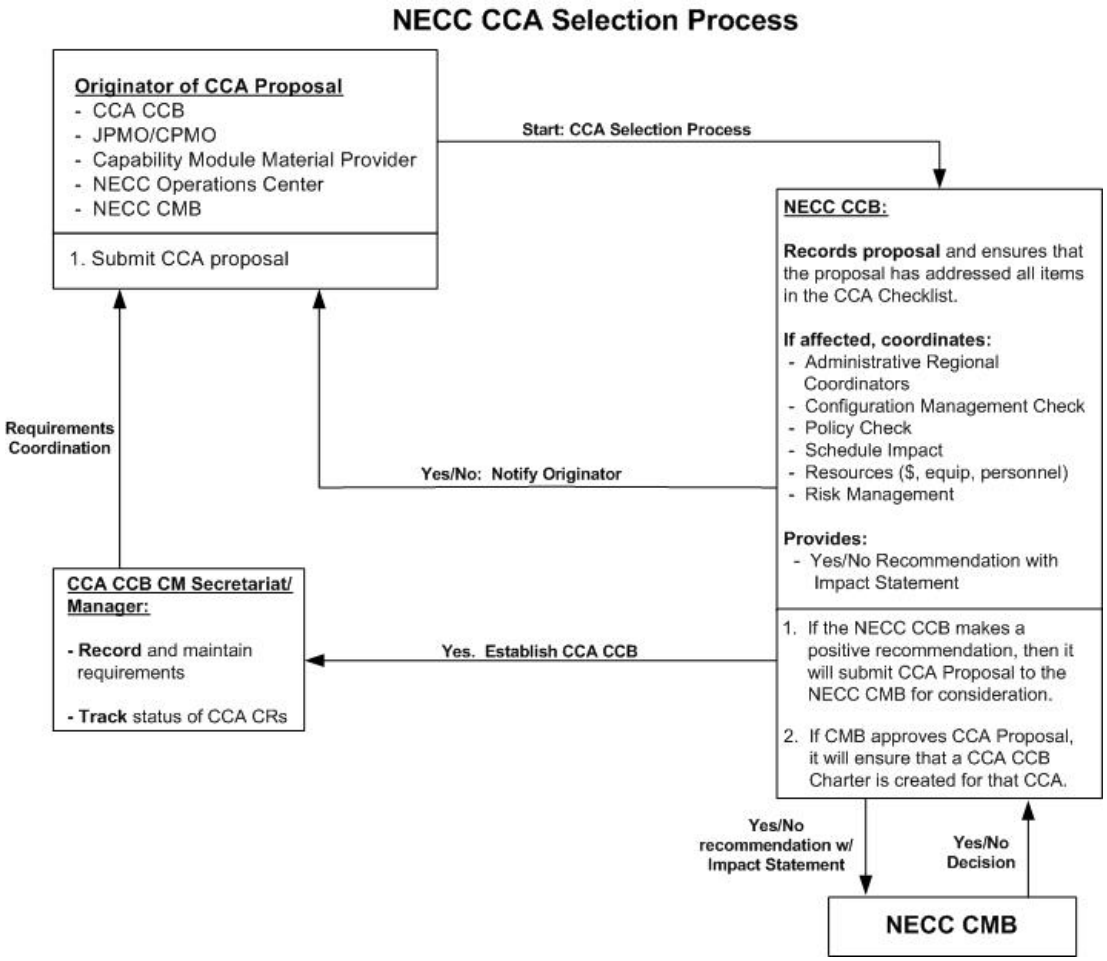

Figure 5: NECC CCA Selection Process

Figure 6 provides a high level view of the CCI Selection process. *Appendix C – Critical Configuration Item Selection Process Checklist* provides a standard checklist for determining whether an item will be considered a CCI. If most of the answers to the questions are "yes," the item will be considered for designation as a separate CCI. If most of the answers are "no," it probably will not be designated as a CCI. However, a single over-riding “yes” may be sufficient to require an item to be separately identified as a CCI.

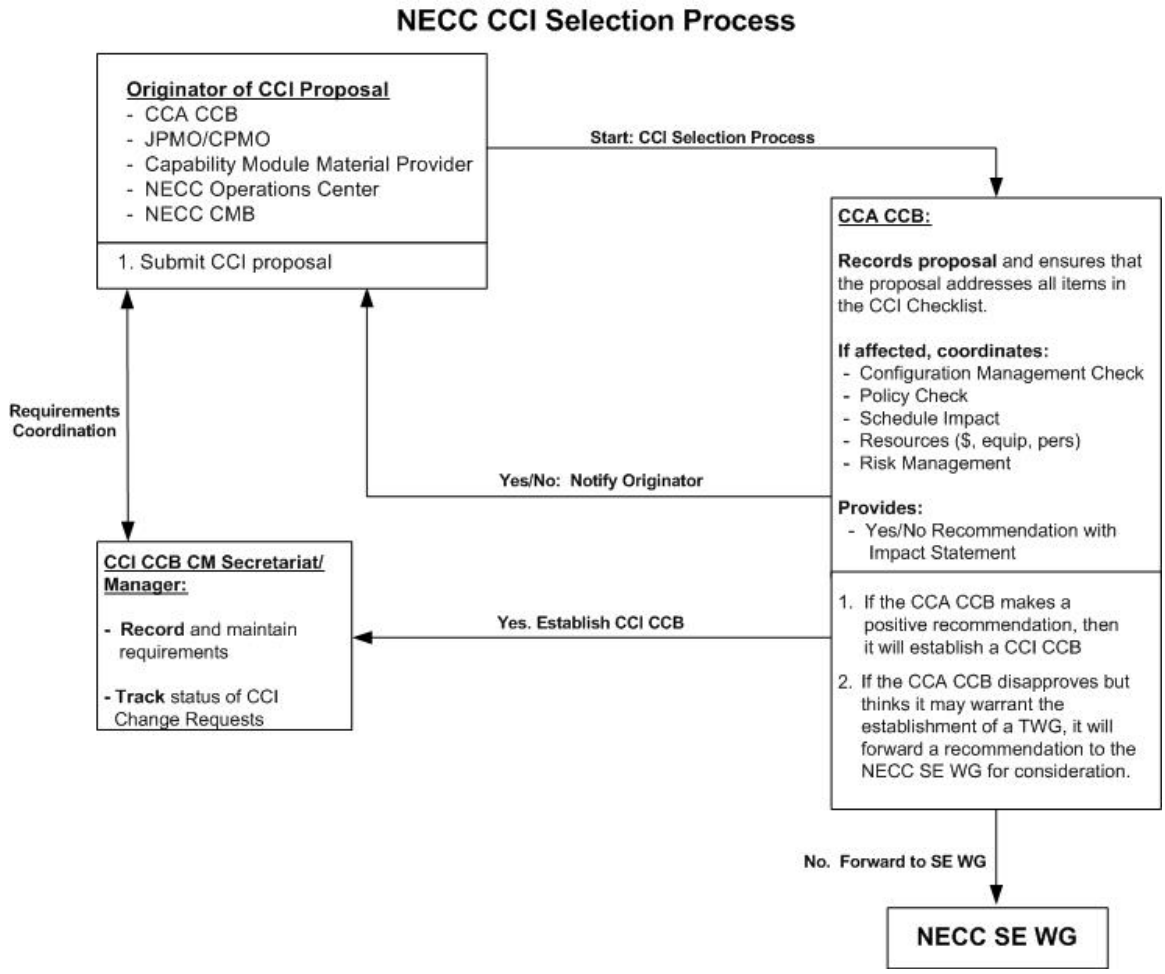

Figure 6: NECC CCI Selection Process

4.2.2 CCA/CCI Registration Process

Initially, the originator will register the proposed CCA with the NECC CMB or the CCI with the relevant CCA CCB. The proposal is registered by submitting the appropriate supporting data as identified in Appendix D.

4.2.3 CCA/CCI Selection Process

The CCA/CCI CCBs, in concert with the NCCB, will recommend to the CMB the depth of control needed for each item and the scope of CCIs that will initially be identified and selected. CCI selection criteria are provided in this section to assist in identifying and selecting candidate items that should be controlled. The following standard object/entity criteria shall be applied to CCI selection:

- Well-bounded and can be managed separately
- Critical to service and functionality
- New or modified technology used in NECC design and development

- Interfaces with other CCIs
- Meets satisfactory procurement conditions: acquisition vehicle in place, budgeted, and committed funds
- Meets logistics and maintenance requirements for expected service life and compatibility with standard installed base.

Each item under configuration control will be classified according to NECC software build and baseline (functional, development, or product). As additional CCI types are required, levels of control shall be defined for each additional type. The NECC Chief Engineer will have final approval of CCIs to be controlled under configuration management. All CCI selections must be traceable to requirements in the Requirements Baseline.

Once the CCI proposal has been received, the NECC CCB review will include the following tasks:

a. Record the CCI proposal
b. Ensure that all CCI Proposal Checklist items have been addressed.
c. Determine the impact (e.g., impact to other CCIs, NECC resources) of the CCI
d. Provide a positive or negative recommendation with an impact statement to the CMB for review and approval.

Once the NECC CMB receives a recommendation from the NECC CCB, the board members will review the proposals and impact statements and make a determination as to whether or not a new CCI is required. CCI proposal decisions will be documented and sent to the NECC CCB for follow-on action.

4.3 Interface Management and Control

This section will be addressed prior to MS C as the program's processes mature and as we gain experience managing the complexities of configuration management in this web-enabled, SOA-based program environment.

5 CONFIGURATION MANAGEMENT ACTIVITIES

CM activities define and control baseline CCIs and provide guidance for reporting and conducting audits on both CCIs and processes. configuration management activities include CI, Configuration Control, Version Control, Audits, and Configuration Status Accounting processes.

One of the most critical CCIs within the NECC structure is the Capability Module. A Capability Module is the collection of one or more services providing operationally useful capability to the Warfighter. An NECC service provides a functional product that is made available to consumers via an exposed network access point. From a consumer's point of view, services are perceived as “black boxes” on the network in that their internal implementation is hidden from the consumer. Because of the critical nature of the services provided (i.e., Capability Modules), configuration management of the Capability Modules is crucial to the austerity of the NECC program.

Capability Modules will evolve through a series of maturation stages using the Federated Development and Certification Environment (FDCE) stages (Figure 7), to the point that it

becomes certified to support Warfighter operations on the GIG. To be certified, a Capability Module must demonstrate the ability to meet defined criteria that address technical maturity, operational relevance, operational utility, net-readiness, and security accreditation. Certification requirements, both technical and operational, increase as a service is moved through the FDCE certification stages from Development to Operations. Hence, CM activities will be applied to each of the Capability Modules at varying degrees as they move through the FDCE stages (described as follows).

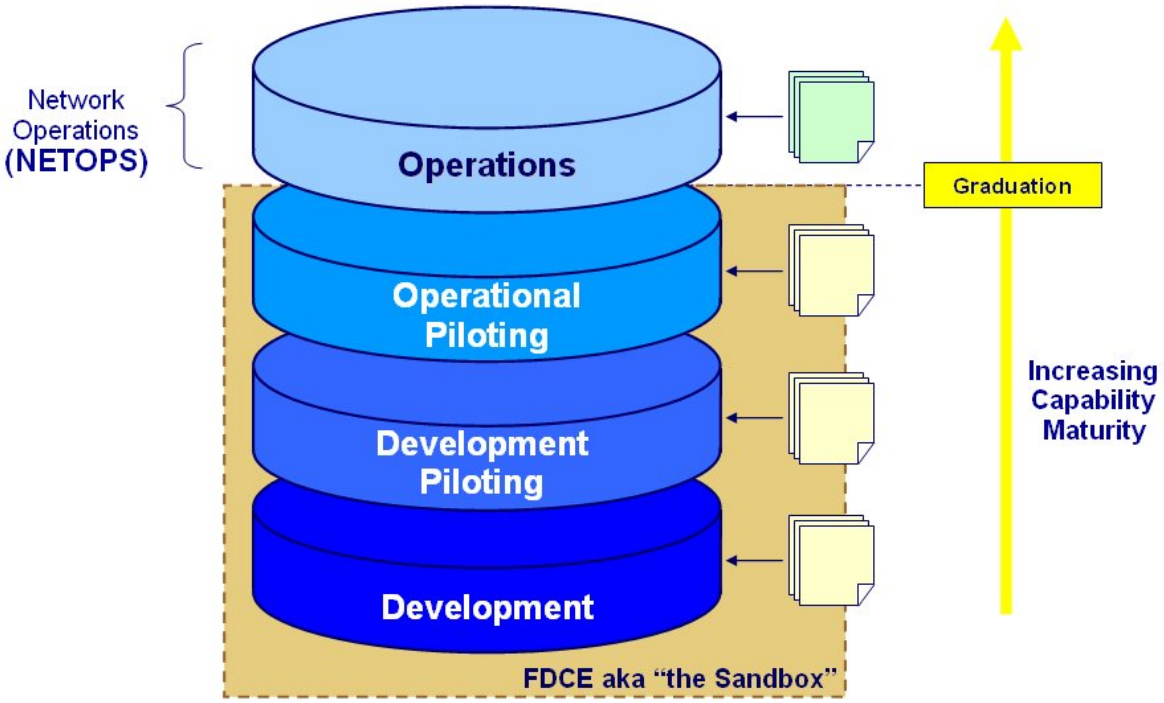

Figure 7: FDCE Stages

Note: While the scope of the FDCE does not include activities involving the Operations Stage, it does encompass certifying services as ready to enter the Operations Stage.

The Development Stage is the entry stage of maturity for Capability Module development and certification. This stage is focused on initial Capability Module development, debugging, and technical exploration. The entrance criteria for this stage, which include limited configuration management controls, will be set as low as possible to minimize the barriers to participation.

The Development Piloting Stage is the second stage of maturity for Capability Module development and certification. The purpose of this stage is to test and certify the net-ready status of Capability Modules. At this stage operational users can begin to use Capability Modules to provide early feedback on operational utility. The entrance criteria for this stage focus on a sufficient level of technical stability and standards conformance to ensure the Capability Module is well behaved. The configuration management controls at this stage shall be enhanced in order to maximize productivity with sound, reliable, and repeatable processes with the intention of maintaining the integrity of the Capability Module baselines.

The Operational Piloting Stage is the final stage of maturity for Capability Module development and certification. The purpose of this stage is to evaluate and certify the operational utility of Capability Modules. At this stage Capability Modules have matured sufficiently to participate in operational exercises and have addressed all security accreditation requirements. The entrance criteria for this stage include net-ready certification and sponsorship from an operational community. CM processes and procedures defined for the Development Piloting Stage should continue to be used. However, the JPMO should review the configuration management requirements to determine if additional controls are required.

5.1 NECC Baseline Definitions

- A baseline is an agreed-to-description of attributes of a product, at a point in time, which serves as a basis for defining change. Further change to an approved baseline can only occur through the formal change control processes.
- The NECC SEP identifies five *Baselines* that are used to manage the evolution of NECC capabilities. These Baseline products provide the mechanisms to perform configuration management across the entire NECC SE process.

5.1.1 Increment Requirements Baseline

Increments are self-contained portions of the system-level CDD. The Increment Requirements Baseline is NECC's version of a traditional System Specification (A-Spec), but enhanced with technical content needed for the development of NECC services. An Increment Requirements Baseline is applicable to each NECC increment and comprises the complete set of systems engineering and architecture products used to define the business (operational) processes, the relevant operational environment, and the C2 requirements derived from the operational requirements of the CDD (as apportioned to the increment). An Increment Requirements Specification (IRS) captures the sum of all increment requirements and will be controlled and managed through a COTS requirements management tool.

5.1.2 Functional Baseline

The NECC Functional Baseline represents the complete set of functional and performance specifications derived from the functional analysis of the business processes (Engineered Mission Threads (EMT)), architecture requirements, and domain-specific functional considerations. The Functional Baseline applies to each increment and describes functional and performance requirements in web service context. This baseline is similar in content and level of detail to the traditional End-Item Specification (EIS), but modified to account for requirements in terms of web service functions and performance requirements instead of overall system functions and performance requirements. The resultant elements of the Functional Baseline are SPSs and are used to define the intended performance of the materiel solutions. The Functional Baseline will be placed under configuration management control and changes to this baseline will be governed through the NECC CCB process. Through this process, the SPS(s) will be tracked to their associated Capability Modules (see following paragraph).

5.1.3 Allocated Baseline

The NECC Allocated Baseline is the set of approved materiel solutions (or Capability Modules) and their allocated SPSs (from the Functional Baseline) plus the addition of implementation and interoperability requirements unique to the domains and architecture considerations. The Allocated Baseline is not established until the JPEO C2C approves the materiel solution (Capability Module). The Allocated Baseline is constructed as the material solutions are approved for development, and is not complete until every functional requirement of the increment has been allocated to an approved materiel solution. Once it is approved for development and enters the Allocated Baseline, the materiel solution is controlled through the NECC CCB and follows configuration management processes as a CCI and contains details similar to a standard sub-system specification.

5.1.4 Product Baseline

The Product Baseline is comprised of the Network Operations (NETOPS) certified "As-Built" materiel solutions (or Capability Modules) and the supporting data package (training manuals, source and object code, and certification and test reports) as defined in the work package used for the development effort. This baseline also contains version-specific information about backward compatibility with other NECC Capability Modules and interoperability with other C2 systems. The Product baseline is constructed continuously as Capability Modules are certified for NETOPS, and are updated as changes to the Capability Modules are made, via CR approval and implementation. The Product Baseline is controlled through the NECC CCB whereas that body will determine the disposition of changes to a Capability Module or forward to the appropriate CCB body for disposition.

5.1.5 Deployed Baseline

Service CPMOs may choose to deploy some or all of the Capability Modules from the Product Baseline, depending on the specific needs at their Service-specific sites. The actual physical distribution of NECC software to enterprise and operational sites is referred to as the updated Deployed Baseline.

5.2 Version Control

Version Control (VC) is the process of managing and maintaining multiple versions of a product. It is accomplished by the use of naming standards, maintaining files in a versioning tool and the use of file tags. Version numbers are used to identify a specific revision of a product. Version Control tracks and maintains the revision history of a product throughout its lifecycle. A revision is a snapshot of a versioned file that can be recreated.

Version tags are used to track software baselines and approved versions of configuration items. Only the Configuration Management Manager has authorization to assign or modify tags. The tags are applied to files and documents in the configuration management VC system. Tags must be used on all CIs. The work products classified as Strictly Controlled CIs are kept under configuration management control throughout the entire program lifecycle. Using the program VC system, each work product will be assigned a tag that corresponds to a baseline.

A complete breakdown of the Naming, Versioning, and Tagging Schemas for the NECC will be contained in the NECC Developers Handbook referenced in Section 1.3.

5.3 Configuration Management Audits

Configuration Management Audits will be conducted periodically to verify the contents of the program repositories, system CCIs and baselines and audit results will be supplied to the JPMO. Configuration audits validate that the design and the final product conform to approved functional requirements, and that changes to the initially approved baseline have been incorporated. Additionally, configuration audits will verify adherence to this CMP, ensure the integrity of a product during the program lifecycle, and ensure adherence to prescribed configuration management processes and procedures. The types of configuration management audits that ensure compliance are – Physical Configuration Audit (PCA), Functional Configuration Audit (FCA), Release Audit, Library Audit, and Process Audit.

5.3.1 Physical Configuration Audit

A PCA is performed before each system is integrated or deployed to ensure the integrity of the system components. A PCA ensures that the "as-built" version of a CI conforms to the technical documentation that defines the item performance. A PCA consists of activities to be preformed prior to the PCA (preparation), during the PCA (actual audit) and following the PCA (reporting). A PCA may also be performed on CIs deployed to a production environment to ensure that they are of the correct version or configuration as defined in the documentation that holds configuration information such as:

a. Software Version Description

b. Platform Configuration document (Deployment Guide)

c. Capability Module Service Specifications

d. All Requirements documents

e. Configuration Management Hierarchy Identification document

f. Hardware Configuration – Minimum Requirements document

g. Installation Procedures

These documents are included in Capability Module, Product, or NECC baselines; therefore, the revision of each document that matches the baseline in production can be retrieved from the Capability Module repository.

5.3.2 Functional Configuration Audit

A FCA verifies that the performance of the CIs comply with all specification requirements. A FCA consists of FCA activities to be performed prior to the FCA (preparation), during the FCA (actual audit) and following the FCA (reporting). Activities prior to the FCA include coordination with the customer, obtaining test verification documentation, CR report, and assembly of additional documentation to support the FCA. Activities during the FCA include supporting the customer in FCA activities, auditing the CIs against the test verification documentation and CRs to verify proper resolution, and creating a list of action items. Activities following the FCA include completing a FCA report detailing all activities during the audit and tracking to completion all action items.

5.3.3 Release Audit

A release audit is performed before each system build to ensure the integrity and readiness of the release. This is a final check to ensure that all steps have been followed in preparing for the release.

5.3.4 Library Audit

A Library Audits are performed on the configuration management repository on a periodic basis to verify the contents are accurate and up to date.

This repository contains electronic Software files, documentation, meeting minutes, etc., and is part of the Configuration Management Tool.

5.3.5 Process Audits

To ensure that configuration management efforts are adequate and completed as detailed in this document, audits and reviews of the processes and products are performed. To ensure that the configuration management program complies with the requirements specified in this plan, an independent audit of configuration processes, procedures, and products is required. Products generated or tracked by configuration management can include:

a. Configuration Status Accounting (CSA) reports

b. Identified CIs

c. CRs

d. Software version releases

e. Libraries

f. Documented configuration management processes and procedures

g. Configuration management review reports

The audit findings are documented in an audit report and provided to the Configuration Management Lead and JPMO. The audit report is used by the Configuration Management Lead to correct deficiencies or identify changes in the configuration management requirements. Examples of correcting deficiencies include updating these processes and procedures, records, configuration documents, repositories, or tools. Identifying changes in configuration management requirements will result in adding, modifying, or deleting a requirement in this CMP.

5.3.6 Configuration Management Reviews

The Configuration Management Manager, or a designated representative, will periodically perform internal reviews of the configuration management processes, procedures, and products. The manager will supply review results to the JPMO. A configuration management review serves as a method to determine how effectively and efficiently the processes and procedures fulfill the requirements as defined in this plan. These reviews also include verification of the products generated by configuration management. Verification is the process of evaluating the products to ensure correctness and consistency with respect to the CMP tasks, processes, and

procedures. The review findings are documented in a report that is used by the Configuration Management Lead to correct deficiencies or identify changes in configuration requirements.

The Lead responsibilities are to execute or assign configuration management personnel to perform reviews and to specify processes or procedures to be reviewed. The review report includes what actions were taken to resolve the deficiency or requirements change. It is filed with the appropriate managers and serves as a record to show that an internal configuration management review was performed and corrective action was taken as required. Review reports may be audited for completeness and accuracy.

5.4 Configuration Status Accounting

The purpose of CSA is to maintain a continuous record of the status of all baselined items. This record is a useful management tool for planning and accomplishing all tasks related to implementing approved changes. The information required for comprehensive CSA includes:

a. Baseline name and version

b. Date each baseline was established

c. Date when each CCI and change was included in the baseline

d. Description of each CCI

e. Change Request

f. Status

g. Description

h. Description of each change

CSA is the recording and reporting of status information related to configuration management activities. CSA is an essential record keeping activity that provides a documented trail as a reliable source of configuration information supporting these activities. CSA provides managers with feedback information to determine whether decisions of the CCB and CMB are being implemented.

The Configuration Management Organization has the prime responsibility for managing, compiling, maintaining, and publishing the detailed CSA reports. The CSA reporting process involves preparation and production of various metrics and status accounting reports using information collected during configuration management activities. CSA results will be reported to the managers, CCB, CMB, and team members involved in, or affected by the proposed actions.

5.4.1 Reporting

The Configuration Management Organization creates reports documenting configuration activities and the contents of the managed baseline report results and sends them to the JPMO via the CMB/CCB. Reports provide status to management ensuring that all CCIs, CRs, action items, and audits are being accounted for and reviewed. The JPMO determines the frequency of CSA reports as well as the distribution and recipients of the CSA reports. Reports include:

a. Approved configuration identifiers

b. CCI Lists

c. Status of proposed and approved changes

d. Status of action items

e. Results of audits

f. CSA reports

g. Configuration Management estimates

5.4.2 Metrics

Configuration management metrics are configuration data collected over the lifecycle of the program. The metrics data will be supplied to the JPMO. The metrics are intended to provide predictive insight and/or historical assessment. The configuration management metrics are managed, controlled, and coordinated by the Configuration Management Lead. Quantitative data related to configuration activities are available to all members. In some instances, it will be necessary for the configuration manager to manually report measurement data.

Metrics presented to the JPMO for evaluation might include:

a. Number of bug reports in Capability Module

b. Number of total changes completed

c. CRs that result in a new feature of the Capability Module

d. Number of CRs outstanding

e. Number of CRs rejected

f. Length of time for CRs to go through the Configuration Management process

g. Number of current versions of a Capability Module and related Capability Packages

h. Modification history for CCIs

6 TRAINING

Training is initially provided to the configuration management group by the appropriate tool vendors and may consist of formal external or internal classroom training, computer-based training, or on-the-job training. The Configuration Management Manager will determine whether the program's Configuration Management Organization has the requisite training. If not, the manager will determine what training is needed. Other responsibilities include identifying, establishing, coordinating, and revising training as required to ensure effective performance of configuration activity by the Configuration Management Organization and related groups.

The manager will train the program’s team members on the CMP and the version control procedures. The Configuration Management Manager will also identify the training needs and make arrangements to conduct training in the following areas:

a. NECC Change Control processes

b. Execution of Change Control using a configure management tools

c. Services/Capability Module Lifecycle

d. Support of Services/Capability Module Lifecycle using a configuration management tool for version control

e. Document librarian processes and procedures (for NON-development environments)

f. Archival processes and procedures

g. Configure Management of Stakeholders as required

7 TOOLS

The configuration management tool used to support the processes shall provide NECC with the necessary capabilities for managing the Configuration Management process and a central location to store program information, CRs, CCIs and Action Items. The JPMO will ensure that the selected configuration tool does not conflict with other tools used by the NECC program. For example, when problems are reported through the Joint Technical Operations Control Capability (JTOCC), those reports can be automatically integrated into the configuration management tool and ensures end-to-end traceability.

APPENDIX A – ACRONYMS

Acronym	Description
A-Spec	A traditional System Specification
C2	Command and Control
C2C	Command and Control Capabilities
C4I	Command, Control, Communications, Computers, and Intelligence
CCA/I	Critical Configuration Area/Items
CCB	Configuration Control Board
CCI	Critical Configuration Item
CDD	Capabilities Development Document
CI	Configuration Item
CM	Configuration Management
CMB	Change Management Board
CMP	Configuration Management Plan
CoE	Centers of Excellence
COI	Communities of Interest
COTS	Commercial Off The Shelf
CPAS	Capabilities Provisioning Activities
CPMO	Component Program Management Office
CR	Change Request
CSA	Configuration Status Accounting
DISA	Defense Information Systems Agency
DoD	Department of Defense
EIS	End-Item Specification
EMT	Engineered Mission Threads
ERB	Engineering Review Board
FCA	Functional Configuration Audit
FDCE	Federated Development and Certification Environment
GES	GIG Enterprise Services
GIG	Global Information Grid
GOTS	Government-off-the-Shelf
IRS	Increment Requirements Specification
JC2	Joint Command and Control

JCCD	Joint Combat Capability Developer
JPEO	Joint Program Executive Officer
JPMO	Joint Program Management Office
JTOCC	Joint Technical Operations Control Capability
MCP	Mission Capabilities Packages
NCES	Net-Centric Enterprise Services
NECC	Net-Enabled Command Capability
NETOPS	Network Operations
NMCS	National Military Command System
NRiD	NECC Requirements Identification Database
PCA	Physical Configuration Audit
PEO	Program Executive Office
PR	Problem Report
SDD	Systems Development and Demonstration Phase
SEP	Systems Engineering Plan
SLA	Service Level Agreement
SME	Subject Mater Expert
SOA	Service Oriented Architecture
SPS	Service Performance Specification
T&E	Test and Evaluation
TD	Technology Development
TDS	Technology Development Strategy
TWG	Technical Working Group
USJFCOM	United Stated Joint Forces Command
VC	Version Control

APPENDIX B – GLOSSARY OF TERMS

Administrative Region Coordinators. A single organization that administers a set of one or more capability nodes in **a Capability Module Administrative Region.**

Capability Module. A collection of one or more NECC services which provide an operationally useful capability.

Configuration Identification. (1) The systematic process of selecting the product attributes, organizing associated information about the attributes, and stating the attributes. (2) Unique identifiers for a product and its configuration documents. (3) The configuration management activity that encompasses the selection of CIs; the determination of the types of configuration documentation required for each CI; the issuance of numbers and other identifiers affixed to the CIs and to the technical documentation that defines the CI's configuration; the release of CIs and their associated configuration documentation; and the establishment of configuration baselines for CIs.

Configuration Control. (1) A systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified. (2) The configuration management activity concerning: the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes; and the implementation of all approved and released changes into (a) the applicable configurations of a product, (b) associated product information, and (c) supporting and interfacing products and their associated product information.

Configuration Item (CI). A Configuration Item is any hardware, software, or combination of both that satisfies an end use function and is designated for separate configuration management. Configuration items are typically referred to by an alphanumeric identifier which also serves as the unchanging base for the assignment of serial numbers to uniquely identify individual units of the CI.

Configuration Management (CM). A management process for establishing and maintaining consistency of a product's performance, functionality, and physical attributes with its requirements, design and operational information throughout its lifecycle.

Critical Configuration Areas (CCAs). CCAs are the mechanism used to manage a wide variety of artifacts that require specialized knowledge and expertise in a particular area. CCAs manage a group of related Critical Configuration Items.

Critical Configuration Items (CCIs). Those configuration items that represent initiatives, functions, processes, and data within the NECC program requiring more focus and management review.

APPENDIX C – CONFIGURATION ITEMS SELECTION PROCESS EVALUATION CHECKLIST

✓	Items to Review
	1. Documented Process
	a. Does the contractor have a documented Configuration Identification process?
	b. Does the contractor follow the documented process?
	c. Are contractor personnel from all disciplines and teams involved in the process informed and knowledgeable about the procedures they are supposed to follow?
	2. Product Structure
	a. Is the product (CCAs/CCIs) structured into a rational hierarchy?
	b. Are subordinate CCAs/CCIs identified at a reasonable level for:
	(1) Specification of and measurement of performance?
	(2) Management of the effects of changes?
	(3) Obtaining spare parts using performance or design documents?
	c. Can the composition of each CCA/CCI be determined from the configuration documentation
	3. Configuration Documentation
	a. Does the contractor's configuration documentation define the performance, functional, interface, and physical attributes of each CCA/CCI ?
	b. Do the performance requirements of the system and/or top-level CCI specifications meet or exceed threshold performance of the Acquisition Program Baseline?
	c. Are all configuration documents uniquely identified?
	(1) Does the identification reflect the source (CAGE code) of the preparing original design activity and current design activity, the type of document, and an alphanumeric identifier?
	(2) Can each document be easily associated with the CCI configuration to which it relates and where applicable, the range of CCI serial numbers to which it applies?
	4. Product Identification
	a. Are all CCAs/CCIs and subordinate parts down to the level of non-reparability assigned individual unique part/item identifiers?
	b. Do the assigned identifiers enable
	(1) Each part/item to be distinguished from all other parts/items?
	(2) Each configuration of an item to be distinguished from earlier and later configurations?
	c. Can the next higher assembly application of each part be determined from the design documentation (including associated lists/records)?
	d. Does the documentation indicate whether CCIs are serialized (or lot controlled)?
	e. Is the common base identifier for serialization/lot numbering always a non-changing identifier?
	f. Is part/item effects to be defined in a manner appropriate for the product type?
	g. When an item is changed to a new configuration, is its identifier altered in both the configuration documentation and on the item itself to reflect the new configuration?

✓	Items to Review
	h. When an existing item is modified, does it retain its original serial number or lot number even though its part/item identifier is changed?(Exception: does not apply to the modification of a part lot or the consolidation of multiple lots.)
	i. Are CCI versions identified and, if applicable, associated to the configuration of the item into which they are to be installed/loaded?
	5. Configuration Baselines a. Are appropriate configuration baselines established and maintained as a basis for configuration control?
	b. Are functional and/or allocated baselines established and maintained for CCAs and CCIs to be controlled by the Government?
	c. Are functional and/or allocated baselines established and maintained for CCAs and CCIs to be controlled by the contractor? By subcontractors?
	d. Is the current configuration baseline for the system and for each CCI easily determinable?
	e. Is an adequate system of release control in place and used for the release of all configuration documents?
	(1) Can the as-released configuration of each CCI be determined?
	(2) Can past configurations be determined? (Applies to both the engineering design configuration and the product configuration.)
	(3) Do release records reflect the authority for changing from one configuration to the next? Do they reference the ECP identifier and Contract Modification (where applicable)?
	(4) Does the release system prevent unauthorized changes to released documents?
	6. Interface Control
	a. For interfaces external to the contractor, are interface agreements established where necessary to document and agree to performance, functional and physical interfaces?
	b. Do CIs being developed by different contractors for the program have well defined interfaces?
	7. Metrics
	a. Are statistical records of document release and other measurable configuration identification actions maintained?
	b. Is the data reduced to meaningful measurement useful in maintaining and improving the process?

APPENDIX – D NECC CRITICAL CONFIGURATION ITEM PROPOSAL

The following is an initial list of data items for a CCI proposal.

a. CCI Title and Description
b. POC data for person submitting the CCI Proposal (Sponsor)
c. Date Submitted for NECC CCB review
d. CCI BM
e. Relationship to the overarching goals of the NECC
f. Existing project CM efforts related to this CCI
g. Trigger for invoking NECC CCB review of other interfacing entities
h. Potential NECC resource impacts
i. NECC Interfaces
j. Appropriate sub-CIs for this CCI.
k. Appropriate configuration controls for this CCI.
l. Appropriate status & accounting procedures for this CCI.
m. Appropriate performance measures
n. Appropriate audit controls for this CCI.

APPENDIX E – NECC CHANGE REQUEST FORM

1. ***CR #*** (should be automatically assigned)		
2.***Date Submitted***		
3.***Title*** Enter a brief, descriptive name of this change request		
4.***Priority***		
5.***Name of Submitter***		
6.***Name of Organization***		
7.***Submitter Contact Info***	***Email:***	***Phone***: (O) (C)
8.***CCA/CCI***		
9.***Change Request Details***		
a. ***Description*** Describe change being requested including description of impacts to existing services if applicable		
b. ***Justification*** Provide a use case for the change being requested.		
c. ***Impact if not implemented***		
d. ***Impact on other services if implemented***		
10.***Change Request Analysis***		
a. ***Scope & Requirements*** Impacts on NECC requirements including whether this is in/out of the scope of the NECC as required		
b. ***Project Risk*** Risks associated with change or over-all impacts of change on project risks		
c. ***Budget*** Include info on impacts to project Budget and details on costs associated		

with this change			
d. ***Alternatives*** Describe alternatives to proposed change			
e. ***Recommendation*** Proposed action based on recommended change and impacts			
f. ***Resolution Description***			
g. ***Request Implementation Activities*** Specific follow-on activities required by the resolution, assigned resources, timeline and other details			
11.***Status***	***Open***	***Closed***	***Deferred***

Priority	Applies if a problems could:
1	a. Prevent the accomplishment of an operational or mission essential capability b. Jeopardize safety, security, or other requirement designated “critical”
2	a. Adversely affect the accomplishment of an operational or mission essential capability and no work-around solution is known b. Adversely affect technical, cost, or schedule risks to the project or to lifecycle support of the system, and no work-around solution is known
3	a. Adversely affect the accomplishment of an operational or mission essential capability but a work-around solution is known b. Adversely affect technical, cost, or schedule risks to the project or to lifecycle support of the system, but a work-around solution is known
4	a. Result in user/operator inconvenience or annoyance but does not affect a required operational or mission essential capability b. Result in inconvenience or annoyance for development or support personnel, but does not prevent the accomplishment of those responsibilities
5	Any other effect