Net-Enabled Command Capability

FEDERATED DEVELOPMENT AND CERTIFICATION ENVIRONMENT (FDCE) BUSINESS PLAN AND CONCEPT OF OPERATIONS (CONOPS)

Version 0.1.5

4 January 2008

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

In Collaboration with the NECC Component Program Manager's for Navy, Air Force, Army, Marine Corps, USJFCOM and DISA.

Disclaimer

This is an informal staff coordination copy. The purpose of this review is to obtain NECC Program Management Direction Team and DISA staff consensus to submit the draft document to the Components for formal review.

This document may be provided to supporting staff activities for information and comment but is NOT for release outside the NECC PMDT or DISA staff.

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (January 2008). Other requests for this document shall be referred to the NECC Joint 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: _____ **Date:** _____

LAURA D. KNIGHT
Joint Program Manager
Net-Enabled Command Capability (NECC)

DRAFT

EXECUTIVE SUMMARY

The Net-enabled Command Capability (NECC) program rapidly develops software command and control (C2) capabilities by building upon and adapting the existing Global Command and Control System (GCCS) Family of Systems (FoS) into a net-centric set of services which operate within a single, joint C2 architecture. An important component of NECC's approach for rapid, agile response to emerging Warfighter needs is the adoption of a new method of piloting, integrating, and certifying capability modules (CMs). This new method is an integral part of the NECC Systems Engineering process and is supported by infrastructure, tools, and process as implemented by NECC's Federated Development and Certification Environment (FDCE).

The FDCE is designed to speed up the process of certifying and accrediting C2 capabilities. The FDCE is a collaborative tool hosted on the Global Information Grid (GIG) that provides a distributed virtual environment to allow NECC stakeholders to remotely monitor, evaluate, and certify CMs as they advance through developmental stages of increasing software maturity. Stakeholders and contributing organizations include Warfighters, Materiel Providers, tool providers, certifiers, developmental labs, and test & integration facilities, all of whom play an important role in CM development and certification.

The FDCE has several benefits, including the following:

- It gives Warfighters an opportunity to participate early in the development process in order to provide continuous feedback on C2 capabilities as they are produced.
- It provides Materiel Providers with access to developer guidance, standard test tools and reference services to include Net-Centric Enterprise Services (NCES).
- It provides access to an array of subject matter experts, including Warfighters, who can also participate in CM development, testing and certification.
- It facilitates early involvement of the various Test & Evaluation and Certification communities.

This document describes the major stakeholders and provides information on how organizations can engage NECC to participate in the FDCE. Appendix A presents an overarching concept of operations that includes delineating the roles and responsibilities for those who participate in the FDCE.

Additional information on NECC can be found at http://www.disa.mil/necc/. For those with access to the Defense Knowledge Online (DKO) Portal, additional information can be found at https://www.us.army.mil/suite/page/453391.

DRAFT

REVISION HISTORY

REVISION NUMBER	REVIEWER / ORG	CHANGES	REVISION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
v0.0.1	JR	Merged CPAS CONOPS and FDCE Business Plan into one document	15 Aug 2007	15 Aug 2007	E. Williams
v0.0.2	EW	Corrected/added appendices; revised figures	27 Aug 2007	27 Aug 2007	E. Williams
V0.0.3	CR, RS, EW	Added Labs & Facilities and FDCE Change Request Form Appendices; included Dave Hirlinger's Piloting Stage Governance input	28 Aug 2007	28 Aug 2007	E. Williams
V0.0.4	EW	Corrected Figure 4; augmented role discussions with content from JST charter, augmented FDCE Stage Promotion discussion w/notional checklists and updated verbiage	31 Aug 2007	31 Aug 2007	E. Williams
V0.0.5	EW/PP/DH	Accept revisions made by Paul Pompier and incorporate new TECC verbiage and figures	17 Sep 2007	17 Sep 2007	E. Williams
V0.0.6	EW	Correct typos, formatting injected during development of V0.0.5	18 Sep 2007	18 Sep 2007	E. Williams
V0.1.0	EW	Incorporate Ms Knight and Mr Kuzma guidance	04 Oct 2007	03 Oct 2007	E. Williams
V0.1.1	RCS	Minor updates	05 Oct2007	05 Oct 2007	R. Siegert
V0.1.2	EW	Incorporate Mr Hall's review comments	10 Oct 2007	09 Oct 2007	E. Williams
V0.1.3	IGJ (BIT)	Reformatted and provided edits. Reset the bullets and numbering, figures and tables; and topic headers for Appendix A. Regenerated the TOC to reflect changes to the document settings.	18 Oct 2007	18 Oct 2007 19 Oct 2007	Issa Jones
V0.1.4	IGJ (BIT)	Inserted the signature block for this document in the Approval page.	23 Oct 2007	23 Oct 2007	Issa Jones
V0.1.5	JB/DH	Incorporated comments from Trailboss.	4 Jan 2008	4 Jan 2008	Dave Hall

DRAFT

TABLE OF CONTENTS

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

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

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

1 INTRODUCTION **1**

1.1 DOCUMENT OVERVIEW 1
1.2 NECC OVERVIEW 2
1.3 NECC CM DEVELOPMENT MANAGEMENT APPROACH 3
1.4 NECC FDCE CERTIFICATION APPROACH 3

2 FDCE SUPPORT PROCESSES **5**

2.1 IDENTIFYING FDCE USERS 5
2.2 FDCE PRODUCTS 6
2.3 OBTAINING AN FDCE USER ACCOUNT 6
2.4 FDCE INFORMATION MEDIA 7
2.4.1 FDCE Working Group (WG) *7*
2.4.2 NECC Working Integrated Product Teams (WIPTs) *8*
2.4.3 Ad Hoc Demonstrations *8*
2.4.4 The FDCE Information Portal *8*
2.5 THE COMMAND AND CONTROL (C2) CAPABILITY CATALOG 8
2.6 THE TOOLS INTRODUCTION PROCESS 9
2.7 THE LABORATORIES AND FACILITIES INTRODUCTION PROCESS 9
2.8 FDCE OPERATIONS 10
2.9 FDCE/NECC HELP DESK 10

3 FDCE INFRASTRUCTURE **12**

3.1 FDCE INSTANTIATION FIELDING AND SUSTAINMENT 12
3.1.1 Fielding *12*
3.1.2 Sustainment *14*
3.1.2.1 IAVA Support 14
3.1.2.2 Infrastructure Upgrades 14
3.1.3 Training *14*
3.1.3.1 Scope of Training 14
3.1.3.2 Roles and Responsibilities 15
3.1.3.3 Techniques and Tools 15
3.1.3.4 Training Prerequisites 15
3.2 FDCE ENGINEERING TEAM 15
3.2.1 FDCE Requirements Management *16*
3.2.2 FDCE Administrators *16*
3.2.3 FDCE Configuration Management *17*
3.2.4 FDCE Quality Assurance *17*
3.2.5 FDCE Testing *18*
3.3 CONTACTING THE PROGRAM OFFICE 18

APPENDIX A - FDCE OVERVIEW AND CONOPS **19**

A.1 FDCE OVERVIEW 19
A.2 FEDERATED DEVELOPMENT AND CERTIFICATION PROCESS (FDCP) 21
A.2.1 Technology Piloting and the FDCE *22*
A.2.2 The TEC Criteria *24*
A.2.3 Tailored TEC Criteria (TECC) *24*
A.2.3.1 Creating TECC and Tailoring the TECC to the CM 26
A.2.3.2 Using the TECC to Select a Materiel Provider 27
A.2.3.3 Configuration Management of the TECC 27

DRAFT

A.2.3.4 TECC Assertions and Validation 27
A.2.3.5 Conduct Maturity Assessment Against FDCE Stage Entrance Criteria 29
A.2.3.6 Apportion Unmet Requirements to Developmental and Operational Test Activities 29
A.2.3.7 Plan Piloting Activities 30
A.2.3.8 Conduct Piloting Activities 30
A.2.4 Certification Entrance Criteria 30
A.2.5 FDCE Stage Governance 31
A.2.5.1 Development to Developmental Piloting 32
A.2.5.2 Developmental Piloting to Operational Piloting 37
A.2.5.3 Operational Piloting to Operations (NetOps) 42
A.2.6 FDCE Portal Functionality 43
A.3 FDCE STAKEHOLDERS - ROLES AND RESPONSIBILITIES 44
A.3.1 Materiel Providers 44
A.3.1.1 What Is a Materiel Provider? 44
A.3.1.2 How Does One Become a Materiel Provider? 45
A.3.1.3 Materiel Provider Roles and Responsibilities 45
A.3.1.4 Oversight and Approval of Materiel Providers 45
A.3.1.5 Materiel Provider Business Processes when Interacting with the FDCE 46
A.3.2 TEC Community 47
A.3.2.1 What Is a Tester/Evaluator/Certifier? 47
A.3.2.2 How Does One Become a Tester/Evaluator/Certifier? 47
A.3.2.3 Tester/Evaluator/Certifier Roles and Responsibilities 47
A.3.2.4 Oversight and Approval of Testers/Evaluators/Certifiers 48
A.3.2.5 Tester/Evaluator/Certifier Business Processes When Interacting with the FDCE 48
A.3.3 Warfighter 50
A.3.3.1 What Is a Warfighter? 50
A.3.3.2 How Does One Become a Warfighter? 50
A.3.3.3 Warfighter Roles and Responsibilities 51
A.3.3.4 Oversight and Approval of Warfighters 51
A.3.3.5 Warfighter Business Processes when Interacting with the FDCE 52
APPENDIX B – USER ACCOUNT APPROVAL PROCESS 53
APPENDIX C – TOOLS ACQUISITION PROCESS 54
APPENDIX D – FDCE TOOLS APPLICATION 55
APPENDIX E – FDCE LABORATORIES AND FACILITIES PROFILE 57
APPENDIX F – C2 CAPABILITY CATALOG METADATA 59
APPENDIX G – ACRONYMS 64
APPENDIX H – REFERENCED DOCUMENTS 68
APPENDIX I – FDCE CHANGE REQUEST FORM 70
APPENDIX J – FDCE HARDWARE CONFIGURATION 72

LIST OF FIGURES

Figure 1: FDCE Stages 4
Figure 2: FDCE Instantiation Overview 13
Figure 3: FDCE Stages 19
Figure 4: FDCE 21
Figure 5: TECC Tailoring Function Model 25

DRAFT

Figure 6: TECC Tailoring and Test Activities Process 26
Figure 7: CM TECC Profiles 27
Figure 8: TECC Assertion and Validation Authorities 29
Figure 9: FDCE Stage Entrance Criteria for a CM and the Decision Makers 33
Figure 10: Promotion from Development to Developmental Piloting 34
Figure 11: Promotion from Developmental Piloting to Operational Piloting 38
Figure 12: Promotion from Operational Piloting to Limited Fielding 43
Figure 13: JFCOM Warfighter Engagement Strategy 52
Figure 14: FDCE Deployment Hardware 73
Figure 15: FDCE Deployment by Enclave 74

LIST OF TABLES

Table 1: FDCE User Account Approval Authority 7
Table 2: FDCE Support Personnel 16
Table 3: Notional Criteria for CM Promotion from Development to Developmental Piloting 35
Table 4: Notional Criteria for CM Promotion from Developmental Piloting to Operational Piloting 39

DRAFT

1 INTRODUCTION

The Federated Development and Certification Environment (FDCE) is a collaborative environment hosted on the Global Information grid (GIG) which consists of processes and infrastructure (software tools and associated hardware) that support all aspects of the software development process (which includes requirements generation, systems engineering and design, software coding, integration and test) as well as certification and accreditation. The FDCE does not provide end user operational command and control (C2) capabilities. The FDCE processes are complementary to the systems engineering process and enable the development, piloting, test, and certification of net-centric capabilities.

The Net-Enabled Command Capability (NECC) program is the next evolutionary step for Department of Defense (DoD)-wide C2 information technology systems. NECC builds upon the existing Global Command and Control System (GCCS) Family of Systems (FoS) technologies and experience to deploy a C2 capability that leverages the DoD adoption of Net-Centricity. In support of the DoD net-centric transformation goals within the C2 domain, and as a key portfolio program within the C2 Capability Portfolio Manager (CPM) landscape, NECC rapidly delivers continuous C2 enhancements to the Warfighter by fielding small, loosely coupled, and militarily useful capabilities. Net-centric transformation requires active participation from an evolving system of people, devices, information, and services interconnected by the GIG. Net-Centric Participants:

1) Support concurrent development and test activities which focus on opportunities for data reuse, standardized data collection, and assessment of individual services for operational effectiveness and suitability
2) Consume or use functions and information rather than implement their own separate systems and services
3) Expose functions and data by making them known to the public and accessible so others can use them
4) Provide standard and registered interfaces for these functions to support discovery and increased use
5) Use standard data formats to facilitate wider consumption and greater utility.

The NECC Program believes it can substantially shorten the development timeline for net-centric capabilities by employing the FDCE to standardize the governance, infrastructure, and processes for developing, testing, evaluating, and certifying these net-centric capabilities.

1.1 Document Overview

This document presents general information and guidelines for participating and collaborating within the NECC FDCE. It provides guidance for stakeholders, including a description of the business rules in place to gain access to the system, guidance for tools acquisition, and other major processes required to work within the FDCE. Stakeholders and participating organizations include, but are not limited to, Warfighters, Materiel Providers, tool providers, testers, evaluators, certifiers, developmental laboratories, and test and integration facilities, all of whom play an important role in Capability Module (CM) development, maturation, and certification. The main sections of the document are:

DRAFT

Section 1: Introduction

Section 2: FDCE Support Processes

Section 3: FDCE Infrastructure.

This document contains links to several NECC workspaces that are located on the Defense Knowledge Online (DKO) Portal (https://www.us.army.mil/suite/page/453391). Users must obtain a DoD Public Key Infrastructure (PKI) user certificate and register to gain access to the DKO Portal.

1.2 NECC Overview

NECC is an evolutionary family of services that merges current and new Warfighter command and control capabilities into a fully integrated, interoperable, collaborative Joint solution. An integral part of this strategy is the transition of the GCCS FoS from its current state of Joint and Service variants to the single Joint C2 (JC2) architecture and capabilities-based implementation of NECC architecture. NECC integrates capabilities into a Service-Oriented Architecture (SOA) that includes applications and databases in accordance with DoD Net-Centric Data Strategy.[2] GIG Enterprise Services (GES) and Net-Centric Enterprise Services (NCES) support NECC by enabling shared access to Service/Agency/Joint-provided services (data sources and applications).

NECC is based on a SOA. The advantages of SOA are achieved by separating the task or function being performed from the software or system being used to perform the task. A CM is a collection of one or more services that provides an operationally useful capability. 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.

The NECC Systems Engineering Process provides guidelines for the nomination and creation of CMs. A CM can be a stand-alone capability or it can contribute to the execution of a mission thread as part of a collection of CMs. NECC services use the core enterprise services provided by the NCES program, and NECC services are implemented in a manner consistent and interoperable with NCES.

The FDCE is the NECC Program's mechanism for accomplishing CM maturation, testing, and certification. The environment is referred to as "Federated" to emphasize that it is not controlled, operated or used by a single organization. For the most part, the NECC Joint Program Management Office (JPMO) neither owns nor operates the facilities or laboratories that contribute to the activities that occur within the FDCE. However, the FDCE processes provide strict governance, administration, and day-to-day management for interconnections with those laboratories when participating in FDCE.

As a virtual environment, the FDCE provides governance, processes, and infrastructure to facilitate the progressive engineering, integration, refinement, testing, evaluation, and certification of selected capabilities in increasingly rigorous stages of maturity, ultimately leading to operational deployment. A capability will accomplish its test and certification at the

[2] DoD Net-Centric Data Strategy, 9 May 2003, URL: https://gesportal.dod.mil/sites/HIRSWG/Issuances/DOD%20Net%20Centric%20Data%20Strategy.pdf

earliest possible opportunity by taking advantage of Capability Provisioning Activities (CPAS) and the FDCE. Essential to this objective is the early and continuous collaborative involvement by the key participants including: the Doctrine, Operations, Training, Leadership, Personnel, Facilities and Policy (DOT_LPF-P), Warfighter, JPMO/CPMO/Materiel Developer, and Test, Evaluation, and Certification (TEC) Communities.

1.3 NECC CM Development Management Approach

The NECC JPMO acts on behalf of the NECC Program Executive Office (PEO) to manage the development of the NECC acquisition strategy, architecture, systems engineering, and migration plans to move C2 systems from current architectures to a net-enabled capability. The NECC JPMO is the lead integrator, responsible for articulating program objectives and status to the NECC Communities of Interest. The JPMO has primary responsibility for NECC life cycle acquisition to include program planning, execution and monitoring to ensure approved functional performance, schedule, and cost goals are met. The JPMO is responsible for acquisition management, resource allocation, budget execution, personnel management, requirements analysis, architecture development, systems engineering, capability development, baseline management, test and evaluation, risk management, configuration management, software sustainment of enterprise-level NECC capabilities, and system support activities. The JPMO coordinates and collaborates with the Component Program Management Offices (CPMOs) to produce NECC capabilities.

Based on recommendations from the JPMO, the PEO funds the CPMOs to develop CMs. For detailed CM development and governance processes, please refer to the NECC Systems Engineering Plan (SEP)[3].

1.4 NECC FDCE Certification Approach

Certification is the NECC quality control approach for ensuring that a maturing CM meets minimum standards of performance, operational utility, net-readiness, interoperability, and security. As described in the TEMP, the Tailored TEC Criteria (discussed in detail in Appendix A) serves as the single integrated point of reference for identification of all promotion requirements between the FDCE stages up to, but not including deployment decisions. Certification occurs when a certification authority or governance body assesses that a CM has met the entrance criteria established for a specific FDCE maturity stage.

CPAS are those activities that various NECC communities perform to develop, implement, test, evaluate, certify, and deliver net-enabled capabilities to the GIG. CPAS incorporates piloting, test, and evaluation activities that use the FDCE. The NECC concept for maturing CMs is to use CPAS through the three FDCE stages, with entrance certification criteria appropriate for the maturity needs of each stage. The FDCE stages shown in Figure 1 are discussed below and in more detail in Appendix A.

1) **Development Stage:** The Development Stage is the entry stage for CM development and certification. This stage focuses on initial CM development, debugging, and technical

[3] Net-Enabled Command Capability Systems Engineering Plan (SEP), Increment 1 Milestone B, Version 1.0 dated 9 August 2007

exploration. Entrance criteria for this stage are set as low as possible to minimize the barriers to participate.

2) **Developmental Piloting Stage:** The Developmental Piloting Stage is the second stage of maturity for CM development, integration, and certification. The purpose of this stage is to test and certify the net-ready status of CMs. The primary objective of this stage is to reduce operational risk. At this stage, operational users can begin to assess CMs to provide early feedback on operational utility. Entrance criteria for this stage focus on achieving a sufficient level of technical stability and standards conformance. This stage is used to test (and integrate as required) the CM with other CMs or systems.

3) **Operational Piloting Stage:** The Operational Piloting Stage is the final stage of maturity for CM development and certification prior to deploying the capability. The purpose of this stage is to evaluate, report, and support the fielding decision. This stage also validates that Joint Warfighter needs are met. At this stage, CMs have matured sufficiently to participate in operational events/experiments and have addressed all security accreditation requirements. The entrance criteria for this stage include net-ready compliance and satisfaction of performance requirements.

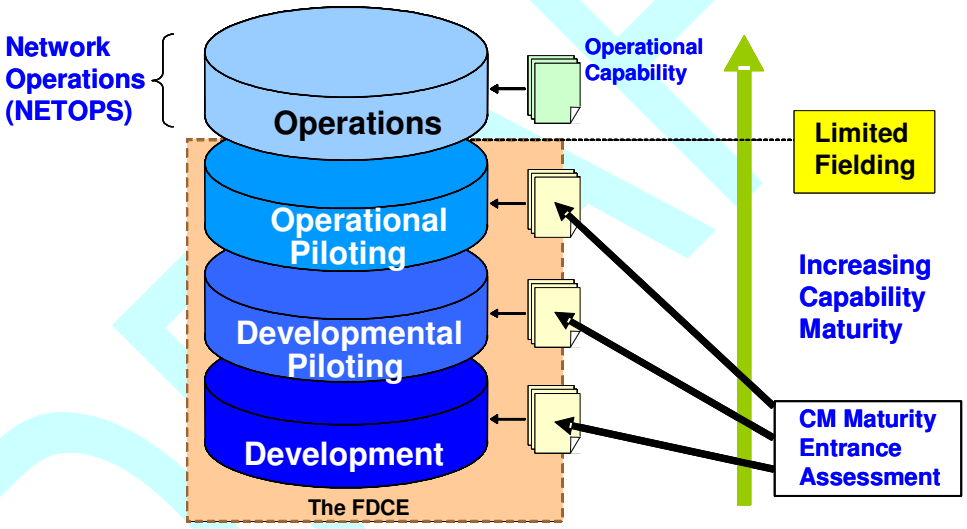

Figure 1: FDCE Stages

To be certified, a CM must demonstrate the ability to meet defined criteria that address technical maturity, operational relevance, operational utility, net-readiness, and security certification and accreditation (C&A). Additionally, the USJFCOM Joint Combat Capability Developer (JCCD) provides an Operational Fielding Recommendation Memorandum for each CM to the Milestone Decision Authority (MDA) that provides recommendations for fielding based on operational and DOT_LPF-P considerations.

Certifying an individual or a system as qualified and ready to perform a set of functions is a well-established concept that has been used successfully for many years. The concept of certifying CMs is similar, yet requires different certification mechanisms. In general, certification requirements, both technical and operational, increase in rigor as a CM progresses through the FDCE maturation stages from Development to Operations. The process of certification acts as an entrance criterion for each FDCE stage. Therefore, while the scope of the FDCE does not

include activities involving the Operations Stage, it does encompass certifying CMs as ready to enter the Operations Stage. The FDCE stages and associated test, evaluation, and certification criteria are discussed in detail in Appendix A of this document.

2 FDCE SUPPORT PROCESSES

2.1 Identifying FDCE Users

The FDCE User Community includes anyone involved in virtually any aspect of a CM life cycle from development through deployment. The following list provides some examples of the types of tasks and activities different types of FDCE users perform:

1) Beginning with requirements definition, the DOT_LPF-P Community uses the FDCE to link to the Joint Combat Capability Developer (JCCD) requirements database and post artifacts such as Capability Definition Packages and Operational Mission Threads.
2) The NECC JPMO and System Engineering (SE) Branch use the FDCE to manage CM Work Package (WP) development by accessing JCCD requirements artifacts and posting SE-generated artifacts such as Engineered Mission Threads (EMTs) and Service Specifications (SPSs). The NECC JPMO also uses the FDCE to plan, execute, and report on CPAS events and to monitor CM development progress.
3) The NECC CPMOs use the FDCE to access CM requirements and specifications documents and draft WPs so that they can respond to JPMO CM calls by making assertions against requirements and posting CM-related artifacts for JPMO review.
4) The Test and Evaluation (T&E) Community uses the FDCE to access JCCD artifacts so it can assist in the development of Critical Operational Issues (COIs) and help assure testability of user requirements. It also uses the FDCE throughout the CM development process to access CM specifications, post and access test plans and reports, monitor CM development and test status, and scope operational assessments and tests.
5) The Information Assurance (IA) Community uses the FDCE to access CM-related documentation required to perform security assessments and to post statuses such as IATOs, IATTs, etc.
6) The Warfighter Community uses the FDCE to gain awareness of forthcoming capabilities and upcoming CPAS events. It also uses the FDCE to access CM-related training materials (both embedded training and training documentation) and provide feedback regarding CM usability and functionality back to the JPMO.
7) The Materiel Provider Community uses the FDCE to register capabilities they are developing, to access requirements they need to meet, to access automated tests, to post documentation and other CM artifacts, and to interface with CMs and services with which they need to integrate or interoperate.

As the FDCE is used more extensively, it is anticipated that more roles will evolve and that existing roles may be refined. For example, the T&E Community may desire or require a distinction between the Developmental Test Community and the Operational Test Community. Detailed information about FDCE roles, responsibilities, and usage is provided in Appendix A to this document, the FDCE Overview and CONOPS.

2.2 FDCE Products

The FDCE provides users with role-specific views, external links, and other services. These are as follows:

- Role-Specific Views – When a user logs on to the FDCE, he/she is shown the information relevant to his/her particular role. For example, whereas testers would see CMs they are responsible for assessing, Warfighters would see CMs available for demonstration.
- Links to External Capabilities and Systems – The FDCE provides linkages to external systems and capabilities as described below:
  - The JSIC Data Collection & Analysis Tool (JDCAT), an automated on-line user survey/questionnaire creation and management tool
  - The JCCD requirements repository
  - The DoD MetaData Repository
  - NCES services (e.g., Service Discovery)
  - The Defense Knowledge On-Line Portal
  - The IA community's IA-CAT tool (eventually to be replaced by eMASS, Enterprise Mission Assurance Support Service)
  - Laboratories and facilities offering up services such as Modeling and Simulation (M&S), network and service load simulations, conformance tools and suites, etc. (For more information about the process for introducing laboratories and facilities into the FDCE process, please refer to paragraph 2.7 and Appendix D of this document.)
  - Deficiency and fault reporting tracking systems and databases, etc.
- NECC/FDCE Organic Services – The NECC JPMO is funding selected tools of wide applicability to the NECC community. One of these, accessible via the FDCE, is the commercial iTKO LISA 4 SOA testing framework. The JPMO is managing a continuing effort to identify tools for potential inclusion in the FDCE infrastructure. More information about the FDCE tool selection process is provided in paragraph 2.8 and Appendix E to this document.

2.3 Obtaining an FDCE User Account

Any user who requires the ability to access the FDCE must apply for and be issued an FDCE User Account. This process allows the JPMO to manage user access and control the actions of approved users.

The FDCE user account controls the actions a user may perform (their role) and establishes ownership (their ownership group) of the various artifacts maintained within the environment. A user's role defines what actions they can perform on an FDCE object (i.e., Introducing a CM, Creating a CPAS event, Validating TEC criteria), while ownership (whether by individual user or Organization/group) defines who may access the object. The JPMO assigns ownership group managers who are responsible for the addition of individual users into a particular group thereby granting access to a particular CM.

To establish an FDCE user account:

DRAFT

1) User applies for an account via the FDCE registration page.
2) The NECC Help Desk forwards the user account application to the cognizant Government Representative.
3) The JPMO/CPMO Representative validates the government sponsorship of the account requestor as well as the need for the specific role requested and processes the application.
4) Users are notified of registration results.
5) Registered users are eligible to be added to ownership groups by the group owner. This is the responsibility of the approved managers for each organization, which manages particular CMs.

In order for individuals to be approved for a role other than Warfighter, one of the following individuals is contacted to verify user requests:

Table 1: FDCE User Account Approval Authority

Name	Role Authorized to Approve	E-Mail Address
Dolgert, Ray	Army CPMO	rdolgert@mitre.org
McGroder, Dennis	Army CPMO	Mcgroder_dennis@bah.com
Redding, Elizabeth	Army CPMO	ERedding@mcdonaldbradley.com
Reginaldi, Lisa	Army CPMO	Lisa.reginaldi@us.army.mil
Hunt, David	DISA CPMO	huntd@pragmatics.com
Wilson, Fred	DISA CPMO	Fred.Wilson@disa.mil
Rivera, Carolyn	Engineer/Manager	Carolyn.Rivera@disa.mil
Morton, Tom	Engineer/Manager	tom@tomorton.com
Hall, Dave	NECC JPMO	David.hall@disa.mil
Flattum, Dave	Navy CPMO	flattum@spawar.navy.mil
Williams, Esther	Tester/Certifier	Esther.H.Williams@saic.com
Park, Jungyoon "Terry"	USAF CPMO	tjpark@mitre.org
O'Riorden, Lynne	USAF CPMO	lynne@mitre.org
Elstad, Brian	USMC CPMO	Brian.Elstad@disa.mil

2.4 FDCE Information Media

There are several means available to parties interested in communicating their requirements to the NECC JPMO or in learning more about the FDCE and its potential utility in a particular context; they are described in the following subsections.

2.4.1 FDCE Working Group (WG)

The FDCE WG meets bi-weekly at DISA's Skyline 7 location with participation open to interested parties associated with the NECC program. To encourage remote participation, the meetings are conducted with teleconferencing and e-collaboration support. The FDCE WG meetings typically focus on development progress, demonstration of enhancements, and communication of new and emerging requirements. Meeting information and briefing materials are posted on DKO in the FDCE Knowledge Center. Systems Engineering Knowledge Center.

2.4.2 NECC Working Integrated Product Teams (WIPTs)

There are a number of NECC WIPTs such as the IA WIPT and the T&E WIPT. The WIPTs typically meet on a monthly basis and focus on a particular subject area (e.g., IA, T&E, etc.). FDCE updates are regularly provided at these WIPT meetings and demonstrations arranged if the membership expresses interest. The WIPTs are also responsible for communicating to the JPMO's FDCE Engineering team any unique requirements for their particular subject area.

2.4.3 Ad Hoc Demonstrations

Requests from external groups (e.g., DOT&E, JFCOM, NII, etc.) for FDCE demonstrations are submitted to the JPMO. Demonstrations may be provided at DISA facilities or on-site at the requestor's facility. These demonstrations comprise another means for interested parties to be introduced to new functionality and provide feedback to the JPMO with respect to usability, enhancements, etc.

2.4.4 The FDCE Information Portal

Every screen (page) of the FDCE contains a "Feedback" link through which users can communicate issues, ideas for improvement, or requests for enhancement. This contextual feedback is tracked and reported on a weekly basis and is one of several methods to convey new requirements to the NECC JPMO's FDCE Engineering team.

2.5 The Command and Control (C2) Capability Catalog

The C2 Capability Catalog is a web-based database of C2 capabilities, hosted at SPAWAR Systems Center, San Diego. Users are required to have a valid CAC with DoD PKI certificate to access the Catalog. Any access requests are submitted using the self-registration process on the site: https://necc.spawar.navy.mil/.

The JPMO implemented this catalog to provide detailed visibility into existing C2 Capabilities. When researching possible solutions which may meet CDD requirements, the capabilities catalog provides a point of reference allowing an efficient, complete process for the archiving and retrieval of known capabilities. Currently, only the GCCS FoS component information is loaded into the database and information is being collected from ACTDs/JCTDs and other C2 systems and programs.

The C2 Capability profile consists of functional, technical, and programmatic factors used to support the transition analysis and decision processes (See Appendix F for details on all available metadata). For FoS transition planning, a profile is populated for each FoS component using the available documents or the information is provided by the appropriate subject matter experts.

The NECC Functionality Transition Plan (FTP) describes the responsibilities of the various NECC organizations with respect to the C2 Capability Catalog. The NECC JPMO is responsible for the generation and maintenance of the C2 Capability Catalog. Data entry/system administration duties are restricted to select JPMO personnel but all other users are permitted access to read and query the database and to create specialized reports based on queries. Read access is granted to designated personnel from USJFCOM, Service PMOs (including NECC CPMOs), DISA GCCS FoS PMOs, and others on a case-by-case basis.

Ideally, to have a capability entered into the catalog, Materiel Providers should have a government sponsor (COCOM, Service, CPMO, ACTD/JCTD) but this is not a hard

DRAFT

requirement. Industry partners with a capability they feel meets requirements of the NECC CDD can submit their capability to the NECC JPMO via an online application.

2.6 The Tools Introduction Process

The NECC program provides a wide variety of tools supporting many different functions. The JPMO has the lead role in the selection, management, licensing, maintenance, funding, personnel support, and help desk support for tools that are being offered to the community by NECC. Additional tools are also made available from external organizations (e.g., the Defense Modeling and Simulation Office could offer up a variety of modeling and simulation tools for use by the NECC Community.) Such tools are hosted and maintained by the external provider organization. The organization providing the tool is also responsible for the accreditation, service level agreements (SLA), personnel support, and Help Desk support for these tools and may charge a fee for use of their tool.

As requirements were developed to support the FDCE community, a NECC tools acquisition process was developed to provide guidelines and structure to create a consistent methodology for evaluating and procuring tools. This process ensures complete and accurate information is captured, reviewed and archived.

The following steps summarize the tools introduction process:

1) Identify Requirement.
2) Complete Tool Acquisition Profile for prospective solutions.
3) Perform Market analysis and meet with the DISA Technical Review Board (TRB).
4) JPMO-assigned evaluation team reviews tool.
5) FDCE CCB makes final decision on tool acquisition.

See Appendix D for further details on the Tool Acquisition Business Process flow. The Tool Acquisition Profile (Appendix D) provides all the core information needed to begin the evaluation process, and is maintained in a database for future reference. The Tool Acquisition Profile is downloaded from the DKO portal or e-mailed to any prospective vendors or interested parties who may not have portal access.

2.7 The Laboratories and Facilities Introduction Process

An underlying tenet of the FDCE is that it is a virtual environment intended to leverage the existing infrastructure (facilities, servers, and networks) of the Materiel Providers developing services for the CPMOs and the developmental laboratories and test facilities performing the developer testing. NECC seeks to leverage this standing infrastructure, augment it where necessary, and provide the infrastructure to support the governance activities taking place within the FDCE. As a resource, this infrastructure plays a vital role to the operation of the FDCE and requires a means to discover the "who, what, where, when, and how" of the resource.

There are three primary resources NECC wants to leverage:

1) People - operators, administrators, validators, and developers who are related to the materiel solution

DRAFT

2) Facilities - plants, equipment, and software available to 'operate' and/or validate a materiel solution

3) Networks - the available connections to the facility.

A NECC laboratories and facilities participation process is being developed to provide guidelines and structure to create a consistent methodology for prospective partners. This process ensures complete and accurate information is captured, reviewed and archived to assist future decisions regarding potential infrastructure augmentation needs to support testing.

The following steps summarize the laboratories and facilities participation process:

1) Identify Need for laboratories and facilities.

2) Prospective Partners complete Profile for proposed solution.

3) NECC JPMO reviews completed Profile for suitability.

4) JPMO-assigned evaluation team reviews laboratory/facility.

5) JPMO makes final decision on Partner participation.

The Laboratory and Facilities Profile (See Appendix E) provides all the core information needed to begin the evaluation process, and is maintained in a database for future reference.

2.8 FDCE Operations

The FDCE Operations department consists of government and contractor personnel that attend to the day to day activities required for the user to successfully use the FDCE and its associated processes. The operations department's goals are to support the long-haul part of the end-to-end FDCE network, including enterprise services and development node integration. The overall goal is to assure effective FDCE operations across data, voice, and other key transport layers. The operations department is responsible for the following activities:

1) Enabling of effective and efficient distributed FDCE operations

   a) Identify and reduce technical obstacles to distributed FDCE activities that support CPAS events.

   b) Accommodate DoD and industry changes that will affect FDCE operations, including net-centric behavior of the GIG, IP Convergence, and IPv6.

2) User Account Creation

3) Tier 2 Help

4) User Role Adjudication

5) Systinet Support -- CM container creation

6) CM Library Support -- per CM (on DKO or DOL)

7) FDCE Demonstration Support

2.9 FDCE/NECC Help Desk

The NECC Help Desk model has been created to provide support for users of the NECC portal and is based on the existing processes developed over the past several years for the Consolidated

C4ISR Help Desk. The NECC Help Desk is an integrated support desk whose mission is to provide 24 hour-a-day, seven day-a-week (24-7) support for customers. The staff uses the BMC Remedy Action Request System (ARS) to track and manage cases by assigning a Case ID to each request. The primary objective of the Help Desk is to document, track, and assign all Trouble Tickets in a timely and efficient manner. The unclassified Help Desk server is accessible via the public Internet and NIPRNet FDCE instantiations using a web browser, and the classified Help Desk server is accessible via the SIPRNet FDCE.

The NECC Help Desk Environment provides overarching troubleshooting support to local Help Desk processes already in place. By providing a net-enabled capability, the NECC Virtual Tier 1 Environment provides support for FDCE specific issues, network outage information, training capabilities, common problem checklist and questionnaires and several other online resources. This mechanism of assisting groups in troubleshooting FDCE capabilities (and other related NECC or CM issues), allows the NECC Help Desk to provide remote support without any need for on-site support. The process is designed to get users in touch with who can solve their problem in the fastest and most efficient way possible.

The NECC Help Desk central access point is not a physical location, but rather a series of physical locations networked together. The infrastructure required to support the NECC Help Desk includes: A central database which has been established to keep continuity of trouble tickets throughout the services and agencies utilizing NECC capabilities and a universal Trouble Management System (TMS) used for trouble tickets (Remedy).

The physical Tier 1 deals with user name, password, and general administrative issues for FDCE users, as well as performing triage on issues with FDCE hardware or software to the next level of expertise. The NECC Help Desk CONOPS provides further details on the management and support plan associated with this process.

The NECC Help Desk can be contacted as follows:

Toll Free: 800-838-1816 (OPTION 4)

Commercial: 843-218-5665

DSN: 588-5665

Unclassified e-mail: NECCHELP@NAVY.MIL

Classified e-mail: **jmcishlp@spawar-chas.navy.smil.mil**

DRAFT

3 FDCE INFRASTRUCTURE

The FDCE infrastructure is the set of distributed hardware and software used to implement Federated Development and Certification processes.

The FDCE infrastructure is physically distributed on the GIG. Only the FDCE administrators require visibility into the physical implementation of the FDCE infrastructure. Network access and role-based permissions are granted to community users who require access to FDCE infrastructure services. These roles correspond to the FDCE user roles of Materiel Provider, TEC Community, and Warfighter.

The infrastructure component of FDCE is an enabler for CPAS. Tools and capabilities include:

1) **Information Portal:**
   a) Watchboard: Provides a management view of CMs maturing in the FDCE to allow oversight of progress, identify schedule and resource issues, and provide metrics on FDCE processes. Additionally, the watchboard provides a quick status of individual CMs as well as the collection of CMs in the FDCE.
   b) User Management: Day to Day management of User roles and account management.
   c) Community Views: Stakeholder views to include Warfighter, Joint System Team (JST), Material Provider, Tester/Certifier and IA.
   d) Workflow Support: A process support that will provide notification to the FDCE user of CM and CPAS activities requiring their attention.
   e) TEC Criteria Management and Tailoring: Specific information regarding the test, evaluation and certification requirements for a particular CM.
   f) Repository: Single source repository that contains all documentation required to support the development, test, monitoring, and CPAS execution of CMs.
2) **Contract Management:** Provides support for generating new contracts, business plans, usage plans, and service level objectives.
3) **Policy Management:** Provides a capability to search for and manage compliance reports, business policies, technical policies, and assertions; validate by running compliance checks; create new business policies; technical policies, and assertions
4) **Information Management:** Provides support for the review and registration of SOA artifacts, integration with the NCES-provided service registry, and the ability to view tasks and reports.
5) **Requirements Management Tool:** RequisitePro
6) **Configuration Management Tool:** SubVersion

3.1 FDCE Instantiation Fielding and Sustainment

3.1.1 Fielding

The FDCE hosting site supports and houses the hardware described in Appendix J of this document. The NECC JPMO is responsible for the operations and maintenance (O&M) of the FDCE development and test suite of hardware and software. The responsibility for O&M of the

DRAFT

NIPRNet suite lies with SPAWAR, Charleston and with DISA Enterprise Computing Center, San Antonio for the SIPRNet suite.

The NECC JPMO is also planning to fund the NECC CPMOs to stand up local instantiations of FDCE nodes as required.

There are three FDCE instantiations provisioned by the NECC JPMO (see Figure 2); they are:

1) FDCE Beta (http://www.fdce.net)
2) FDCE NIPRNet (https://fdce.sspl.disa.mil)
3) FDCE SIPRNet (https://fdce.osf.disa.smil.mil)

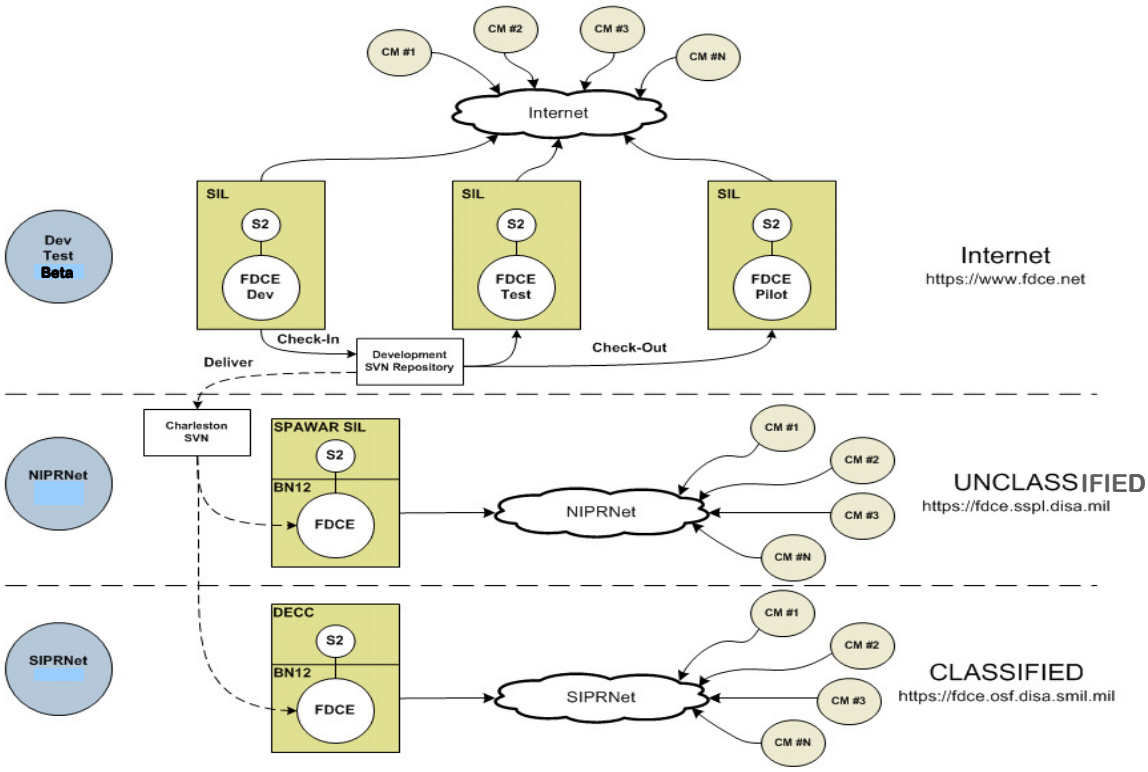

Figure 2: FDCE Instantiation Overview

NECC utilizes FDCE NIPRNet and FDCE SIPRNet as the repository for information relating to CMs that are being developed for the program. FDCE NIPRNet and FDCE SIPRNet are used by various communities to track status and maturity, to conduct testing and piloting, and to post CM documentation and artifacts. Information entered into FDCE NIPRNet and FDCE SIPRNet is persistent and backed up on a regular basis as protection against data loss.

FDCE Beta is set up as an "early look" for emerging functions and demonstrations and as a training ground for users needing to “try-before-they-fly” in the NIPRNet and SIPRNet FDCE. The FDCE Beta site should be considered an FDCE User Free Play site. No government information should be entered into the FDCE Beta site and information entered into the FDCE Beta site is not persistent or backed up.

3.1.2 Sustainment

A critical part for the successful sustainment and support of any system is the ability to address known IAVAs and respond to updates to the underlying infrastructure. The NECC JPMO, supported by the FDCE Engineering team, has a process in place to ensure that the FDCE Infrastructure remains current with the latest vulnerability bulletins as well as product upgrades.

3.1.2.1 IAVA Support

With the increase in the number of COTS/GOTS products being introduced in the development of software applications it is critical to stay abreast of any security threats or software vulnerabilities. The Engineering team is responsible for the monitoring of IAVA bulletins and reacting appropriately to any perceived threats.

The following steps summarize the process that is in place to manage and address IAVAs that may affect FDCE:

1) FDCE IA engineers receive IAVA/IAVB/TA notices via e-mail from DoD-CERT.
2) IAVAs trigger "open" findings in DISA's Vulnerability Management System (VMS).
3) IA engineers review details and download applicable patch at: http://iase.disa.mil/index2.html.
4) IA Engineers acknowledge IAVA notification in VMS.
5) IA Engineers coordinate with Configuration Management / Developers to identify and assess potential application impacts.
6) Review of IAVA patch issue and approval to install is received from the FDCE ERB and CCB.
7) IA engineers install patch and run self-vulnerability assessment.
8) IA Engineers update VMS and/or POA&M.

3.1.2.2 Infrastructure Upgrades

The FDCE Information Portal depends on a number of COTS products that shall undergo product enhancements and bug fixes. These products include (but are not limited to) a relational database, an application server, and a supporting artifact repository. Any upgrades or modifications to the supporting FDCE Infrastructure are treated as a part of a major FDCE Infrastructure release and are scheduled with an appropriate development/delivery cycle. These updates undergo the same scrutiny and review by the ERB and CCB as any new requirement to the FDCE Information Portal. Any emergency fixes are handled like the IAVA process described in the previous section.

3.1.3 Training

3.1.3.1 Scope of Training

The FDCE Training plan provides the necessary understanding to support the NECC CM development & certification lifecycle using the FDCE and its associated tools, tailored to the tasks the user is required to perform. This training includes an overall understanding of the NECC software development paradigm, starting with the development of a CDP, definition of

DRAFT

CMs, maturing of capabilities via the development, piloting and T&E processes, and what is required to promote capabilities between FDCE stages and ultimately to an operational status.

The training plan focuses on End User training (Role-based/Business Process-based training), but also has additional support for the Super User/Administrator.

3.1.3.2 Roles and Responsibilities

The JPMO, in conjunction with the FDCE Engineering team, develops a curriculum and supporting materials for a formal FDCE training capability. These classes and material augment existing documentation such as the NECC FDCE Quick Reference Guide, the NECC FDCE Operating Instructions, and the FDCE's on-line Help capability. The FDCE Engineering team is responsible for conducting any required formal classroom training.

3.1.3.3 Techniques and Tools

The FDCE training class consists of a hands-on practical session and classroom lecture which covers the full gamut of information needed to understand both the overall environment in which NECC is operating and the operation of the FDCE portal application and any associated tools.

The training may be performed at any site that is able to provide internet connectivity, PC workstations, and projection capability. If training is to include actual real world access to data, then NIPRNet or SIPRNet access would be required depending on the capabilities involved.

Training Materials include FDCE Operating Instructions FDCE OI Document on DKO, the FDCE Training Class Presentation, and supporting training documentation.

3.1.3.4 Training Prerequisites

Any attendees of the NECC FDCE Training program must meet the following prerequisites:

1) Obtain government sponsor approval.
2) Apply for and obtain and FDCE User account.
3) Review the FDCE Quick Reference Guide and the NECC FDCE Operating Instructions.

3.2 FDCE Engineering Team

The FDCE Engineering team is involved in the full software lifecycle of this project. This includes the requirements gathering phase, software design, implementation, test, and fielding/sustainment phases of this effort.

The following roles make up the current FDCE Engineering team:

1) FDCE Project Manager
2) Chief Engineer
3) Technical Lead
4) Software Engineer(s)
5) Subject Matter Experts (e.g., Test and Evaluation, Certification and Accreditation, etc.)
6) Requirements Management

7) Administrators

8) Configuration Management

9) Quality Assurance and Testing

The estimate of FDCE support personnel requirements shown in Table 2 was developed for the NECC CARD (Cost Analysis Requirements Description (CARD), 20 Jun 2007); it summarizes projected DISA FDCE staffing requirements for FY08 – FY10. Personnel requirements are in addition to the current positions identified above.

Table 2: FDCE Support Personnel

DISA PERSONNEL SUPPORTING THE FDCE

DEVELOPMENTAL PILOTING TEST MANAGEMENT	**MIL**	**1**	**E7**
OPERATIONAL PILOTING TEST LEAD	**CIV**	**1**	**GS13**
OPERATIONAL PILOTING TEST MANAGEMENT	**MIL**	**1**	**04**
CONFIGURATION MANAGEMENT	**CIV**	**1**	**GS12**
SYSTEM ADMINISTRATION	**CIV**	**1**	**GS12**
SYSTEM ADMINISTRATION	**CIV**	**1**	**GS12**
CONFIGURATION MANAGEMENT	**CTR**	**2**	

3.2.1 FDCE Requirements Management

The FDCE Engineering team has developed and established a baseline set of FDCE Infrastructure requirements which as been approved by the FDCE Configuration Control Board (CCB). The FDCE Requirements Document also depicts the allocation of the requirements to the FDCE Build schedule. When changes to the existing requirements or new requirements are identified, they are documented via the FDCE Change Request Form and brought before the FDCE CCB for discussion and subsequent analysis, approval, or disapproval. As new requirements are approved for implementation, they are incorporated into the Requirements Document and the document version reflects the new baseline.

Any member of the project or client staff may submit a change to the current FDCE requirements. The form can be downloaded from the FDCE Reference Library link in the FDCE; for your convenience, it is also provided as Appendix I to this document. Completed forms should be submitted to the FDCE CCB Secretariat at: harkinsj@saic.com.

3.2.2 FDCE Administrators

FDCE Administrators operate and maintain the FDCE infrastructure, configure and manage the software and tools used to implement the FDCE processes, and provide technical and procedural help to the broader capability provisioning community.

DRAFT

The NECC JPMO is responsible for the Administration of the FDCE. Responsibilities include:

1) Database Management
2) Administering the creation of individual and group accounts and controls access rights for those accounts
3) Certification and Accreditation
4) Document Management/Librarian
5) Data Repository Management
6) Configuration Management
7) Development and maintenance of FDCE related Documentation, e.g., User Guides, Operating Instructions

3.2.3 FDCE Configuration Management

The FDCE Configuration Management strategy allows the production of FDCE software by a distributed Engineering team while imposing controls assuring the integrity of that software through the change control process. This process includes the baselining of the approved software builds within the configuration management tool environment, release of the deliverable products, and the deployment of applications. The web-enabled configuration management software repository is hosted by SPAWAR System Command (SSC) Charleston. This repository also hosts all FDCE CCB approved baselines. Please refer to the NECC Configuration Management Plan for more information.

FDCE development is an iterative process and is requirements-driven. The FDCE Project Manager determines that a build within the development environment is ready for installation on the testing server as a candidate version release.

Candidate Builds undergo formal testing and test results drive additional development to fix problems or bugs; or approval by the FDCE Engineering Review Board (ERB) indicating the build is ready for CCB approval of its release to the Beta and/or NIPRNet and SIPRNet sites.

3.2.4 FDCE Quality Assurance

Need Tom/Jon Morton (Chief Engineer) input here and in Test section (3.2.5).

FDCE software quality assurance (SQA) is an umbrella activity that is applied throughout the entire software development process - monitoring and improving the process, making sure that any agreed-upon standards and procedures are followed, and ensuring that problems are found and dealt with. It is oriented to prevention and is comprised primarily of verification and validation activities.

Verification addresses "Are we building the right system?", that is, are user requirements adequately addressed? Validation addresses the flip side, i.e., "Are we building the system right?" The latter activities focus on standards conformance, reliability and maintainability, error trapping and handling, etc.

DRAFT

3.2.5 FDCE Testing

FDCE software testing involves operation of the FDCE under controlled conditions and evaluating the results. It is focused on 'detection'. Testing is used at key checkpoints in the development process to determine whether objectives are being met. When the design is complete, coding follows and the finished code is then tested at the unit level by each programmer; at the component level by the group of programmers involved; and at the system level when all components are combined together. Throughout this internal testing, the FDCE is made available to alpha and beta users so they can assess it for usability.

Since the objective of FDCE prototyping activities to date was on defining and exercising processes vice development of a production version. Thus, testing was not as exhaustive as it could have been. For future FDCE development, there will be more emphasis on these basic validation test strategies:

1) Unit Testing
2) Integration Testing
3) System Testing
4) Performance Testing
5) Alpha Testing
6) User Acceptance Testing
7) Installation Testing
8) Beta Testing

Ultimately, the intent of FDCE software testing is to determine whether the system meets specifications and to determine whether the system meets business and user needs. The test burden is shared by the FDCE engineering team and a variety of users including representatives from DISA's Test & Evaluation Management Branch, the TEC Community at large, JFCOM & JSIC, the CPMOs and their Materiel Developers, and NECC JPMO representatives.

3.3 Contacting the Program Office

For general information about NECC, go to the following:

1) Internet: http://www.disa.mil/necc/

   For additional information and program documentation, go to the Defense Knowledge Online Portal NECC Home Page on DKO. Account registration information can be found at: https://www.us.army.mil/

2) NIPRNet: https://www.us.army.mil/suite/page/453391
3) SIPRNet: https://gesportal.dod.smil.mil

DRAFT

APPENDIX A - FDCE OVERVIEW AND CONOPS

A.1 FDCE OVERVIEW

The FDCE is a virtual and collaborative environment that addresses the challenges associated with developing and certifying net-centric capabilities in support of today's Warfighters. The FDCE provides the governance, processes, and infrastructure for moving a CM through the maturation processes by allowing all the capability provisioning players to participate via the network. In other words, the FDCE facilitates the progressive refinement, testing, evaluation, and certification of capabilities in increasingly rigorous situations leading to an operational implementation. The FDCE is portrayed graphically in Figure 3.

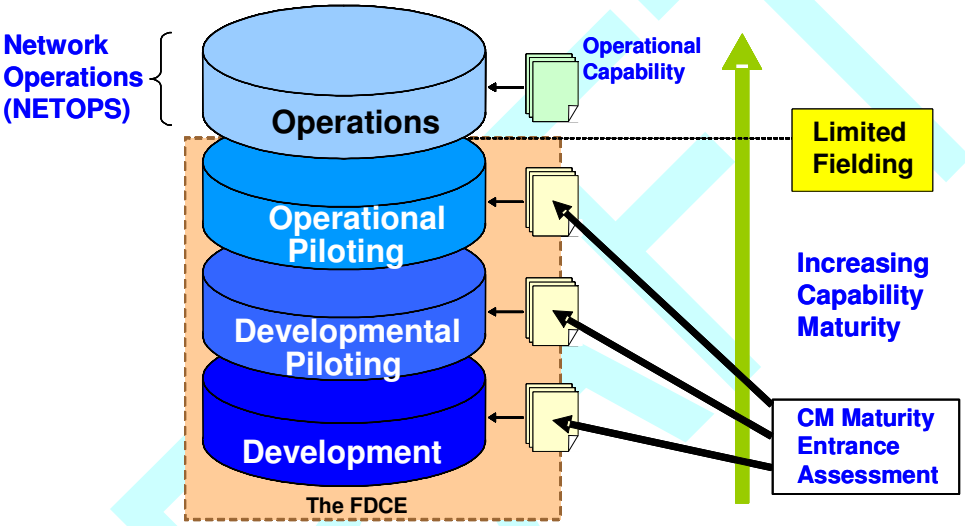

Figure 3: FDCE Stages

The FDCE is a development, T&E, and certification management tool that supports the CPAS process. The FDCE provides the environment that facilitates testing for integration and interoperability with all Service/Component platforms in accordance with (IAW) DoD Directive (DoDD) 5100.30 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E and NECC TEMP. The NECC JPMO, as the technical standard configuration control manager, uses the FDCE to publish and support the enforcement of technical and operational standards governing CM development. In addition, The FDCE provides a CM technical parameter configuration control database to ensure all CMs use a common technical view standard that is flexible to support future technologies, and also to support legacy technologies for information exchange compatibility. The FDCE tracks and displays CM certifications for each stage providing real time management of CMs to support activities and events as shown in Figure 4. CMs can enter at different stages of the FDCE based on a maturity assessment, which is conducted by the NECC JST. Once a CM has completed all of the certification and testing requirements for the Operational Piloting stage, a CM Assessment Report (CMAR) is provided to the MDA (or designee) to support a Limited Fielding decision. The CMAR is the equivalent of a formal Operational Test (OT) report. In addition to test results, the CMAR also documents

the results of all CM certification activities including Network Operations (NETOPS) and Net-Ready Key Performance Parameter (NR-KPP) certifications.

DRAFT

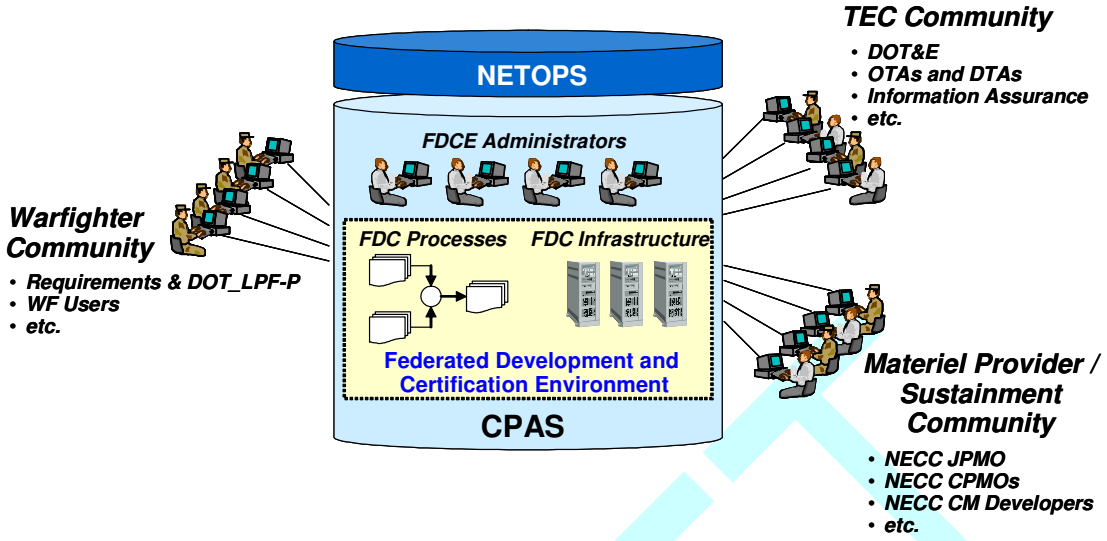

Figure 4: FDCE

To accomplish this role, NECC has structured the FDCE by creating a set of processes and the underlying infrastructure needed to support conducting net-centric CPAS. As structured by NECC, the FDCE can be separated into two components:

1) **The FDCE process** is the set of procedures used by the NECC community to develop, implement, test, evaluate, certify, and deliver CMs through the maturation processes. The FDCE is analogous to our natural environment. The natural environment consists of the external conditions, resources, stimuli etc. with which an organism interacts to grow from its embryonic state to a mature state. Likewise, the FDCE consists of the external conditions, resources, stimuli, etc. to grow a capability module from a paper requirement in the Capability Development Document (CDD)/Capability Definition Package (CDP) to a fielded material solution.

2) **The FDCE infrastructure** is the set of distributed hardware and software that is used to implement federated development and certification (FDC) processes; manage the certification status of CMs; and provide the Materiel Provider community with web-based screens for conducting CPAS events.

It is important to understand that from a Materiel Provider perspective, the FDCE is a virtual environment, not a physical place. For example, the Navy might create a CM for Waterspace Management that is operated from SPAWAR Systems Center, San Diego. By exposing the Waterspace Management CM to the GIG and registering it with the Enterprise Service Registry using the FDCP, the CM becomes "part" of the FDCE.

A.2 Federated Development and Certification Process (FDCP)

The FDCP is the set of procedures that are used to develop, implement, test, evaluate, certify, and deliver CMs to the Warfighter through the maturation process.

Establishment of the FDCP, including the necessary governance mechanisms, is done via a community-wide activity led by the NECC JPMO and in support of the USJFCOM JCCD Process. The FDCP addresses procedures for:

1) Registering new CMs
2) Reviewing and providing feedback of CMs from a Warfighter.
3) Establishing TEC criteria for the CM
4) Submitting CMs for certification
5) Obtaining the certification status of CMs
6) Creating CPAS events to test and evaluate CMs
7) Reporting the results of CPAS events

One of the advantages of the FDCP is the ability to facilitate early Warfighter involvement in the CM development process. Previous system development processes involved the user at the requirements development stage and generally did not get the user involved again until the very end of the development cycle at acceptance testing. This gap often stretched out over several years. In the dynamic environment of modern military operations, little remains constant for very long. Threats and requirements evolve at a rapid, unpredictable pace, and capabilities developed without continual end-user involvement may be obsolete before they are fielded. The FDCE enables continual user involvement throughout the development lifecycle through User Free-Play, Capability Provisioning Events, Operational Concept Exercises, and major military operational exercises. Involving users early and often in the development process ensures that capabilities meet the requirements of end users by providing timely feedback to the CM developers. It also ensures that users' expectations remain consistent with the capabilities of the CM.

A.2.1 Technology Piloting and the FDCE

Piloting is a means of providing an environment where technology demonstrations, experimentation, and T&E can be conducted in a realistic SOA environment. Each stage of the FDCE has a layering of certifications that enable testing in different environments ranging from limited access to full operationally representative environments. To bring discipline to this piloting framework, CPAS were established. CPAS are a set of formal net-centric processes for maturing NECC-developed CMs from initial conception to a state where they are ready to support military operations on the GIG. The main idea behind CPAS is to create a mechanism that supports and enables developers and testers to deliver, test, and certify all the C2 products in a rapid, continuous, cyclical manner. This includes improvements which take advantage of emerging technologies and operational lessons learned. The CPAS concept brings together Warfighters; the JCCD; materiel developers (i.e., engineers, software developers, and integrators); testers; evaluators; and security accreditation experts as capabilities are matured.

A key aspect of the CPAS model is the concept of accelerating the development, certification, testing, and evaluation of new C2 capabilities using technology piloting. CPAS, via the FDCE, makes not yet fully matured capabilities available to interested parties for experimentation, testing, and evaluation. Unlike capability demonstrations, which are of limited and short duration, piloted capabilities must be made available on an ongoing and extended basis.

DRAFT

When CMs participate in piloting events, the purpose is threefold: 1) it gives potential users an early look at emerging capabilities; 2) it supplies Materiel Providers and developers feedback on the usability and correct functioning of the CM; and, 3) it provides documented results and other artifacts for the test community. To ensure that objectives are met, careful management is required for CM participation in a piloting event. User expectations with regard to the CM's functionality must be carefully scoped. If users expect too much, resulting evaluations will be unfairly judged. If users expect too little, the CM may not be fully exercised during the pilot.

In addition to managing expectations with respect to CM functionality, it is necessary for developers and Materiel Providers to understand the conditions under which the CM will be evaluated and how closely those conditions mirror the expected operational environment. This information is vital to correctly interpreting the data gathered during piloting events, and helps to ensure that valid conclusions are drawn from the data.

NECC uses multiple piloting methods to encourage early and regular interaction between developers and end-users. Piloting method(s) selected will likely differ from activity to activity. The methods selected are intended to be flexible and malleable to the needs of a specific CM. As discussed in the *NECC I&TP CONOPS*, I&TP CONOPS on DKO, there are three primary types of piloting methods used to support the rapid provisioning of NECC C2 capabilities onto the GIG:

1) **User Free-Play (UFP)** events are a type of piloting activity where individual Warfighters, requirements/doctrine providers, and other stakeholders evaluate CMs through unstructured free play within the FDCE. This type of event, similar to alpha or beta testing may be planned, scheduled, and executed with little lead time and low overhead cost thus allowing quicker feedback on NECC capabilities. The duration of survey data collection will define the duration of the UFP event. The user surveys will provide the feedback mechanism and will be qualitative in nature.

   UFPs can be implemented for a CM in any of the Development, Developmental Piloting, and Operational Piloting stages of the FDCE. These events are primarily intended to introduce emerging NECC capabilities to warfighters early as alpha/beta users and provide capability feedback in a less formal environment to provide CPMOs and materiel developers with user feedback on capabilities being developed. There are two classes of UFP events:

   a) **DT Class** – a UFP planned and conceived to obtain Warfighter feedback relevant to specific technical (functional) or capability performance characteristics of a Web service or CM.

   b) **OT Class** – a UFP planned and conceived to obtain Warfighter feedback relevant to specific suitability and performance characteristics of a Web service or CM. It can also be structured to assess a set of operational test class goals/criteria, typically performance and suitability characteristics with MOPs and Measures of Suitability (MOSs) to support a CM fielding decision.

2) **Capability Provisioning Events (CPEs)** focus more on testing and evaluating capabilities. The objective of a CPE is to clearly articulate assessment objectives and collect quantitative and qualitative data that address these objectives. These events are intended to be more narrowly focused than OCEs and to require much less lead-time to prepare. However, this concept of a lightweight and agile process model is balanced by necessary rigor and

repeatability, evidenced by a process framework supported by planning, review, and assessment artifacts.

A CPE is implemented in the Development, Developmental Piloting, or Operational Piloting stages of the FDCE. The *NECC I&TP CONOPS* describes each of these FDCE Stages and how piloting fits into each.

The entire NECC JPMO team –SE, I&TP, T&E – as well as the JCCD and JST communities will be involved in determining when a CPE will be required as well as the objectives of the CPE. Criteria and risk assessment matrices from the JST determine the assessment objectives which define the characteristics and scope of a CPE. In the absence of JST governance, objectives will come from other sources (e.g., SLAs, WPs, etc.).

3) **Operational Concept Events (OCEs)** are a type of piloting activity primarily focused on evaluating new operational concepts with a secondary objective of evaluating new C2 capabilities. These events will allow materiel providers and test teams the opportunity to evaluate capabilities in the most realistic operational testing environment available. These events will normally occur in joint or service-specific exercises/experiments.

An important role that FDCE plays in CPAS piloting is to provide the mechanisms, tools, and collaboration support necessary to support the rapid piloting timelines of these three methods.

Note that while OCEs are an important part of piloting at the end of the scale, it is critical to establish UFP and CPEs as the center of gravity for NECC piloting and OT.

A.2.2 The TEC Criteria

The TEC Criteria database is an exhaustive inventory of possible criteria that is tailored during the systems engineering (i.e., Step 4 through Step 6 processes) to produce a specific, configuration-managed, set of criteria that apply to a particular CM. The database comprises the requirements found in authoritative documents, such as the Capability Development Document (CDD) and Capability Definition Package (CDP) as well as DoD policies governing Net Ready Key Performance Parameters (NR-KPP), Information Assurance (IA), and DoD Information Technology Standards Registry (DISR). However, these standing criteria are not subject to the dynamics of the systems engineering process. As the engineering process matures the WP for a particular CM, the criteria found in the Operational Mission Thread (OMT), Engineered Mission Thread (EMT), Service Performance Specifications (SPS), Operational Test requirements, and the DOT_LPF-P applicable to that CM are added to the tailored criteria set. These criteria may also be added to the TECC database for reuse by other CMs. This process is detailed in paragraph A.2.3, Tailored TEC Criteria. In all cases, criteria are mapped back to their authoritative source.

A.2.3 Tailored TEC Criteria (TECC)

The TECC is the center of gravity for any CM. It ties the systems engineering effort to independent verification and validation (IV&V) efforts including test and evaluation (T&E). As implemented in the FDCE TECC Administration Tool, the TECC affords the following advantages:

1) Provides a discrete, configuration managed set of criteria the materiel developer can use to build the materiel solution.

2) Provides a means by which unmet requirements can be apportioned to future developmental and operational test events by focusing on the relevant criteria for a CM at a particular stage of maturity.

3) Provides a method by which program management can monitor maturation of the CM.

4) Provides a historical record of the disposition of each criterion including decisions to re-test, defer, or waive criteria that failed during test or could not be met for other reasons (e.g., the required technology is not yet sufficiently mature).

As shown in Figure 5, the TECC tailoring process is influenced by various inputs, mechanisms and controls.

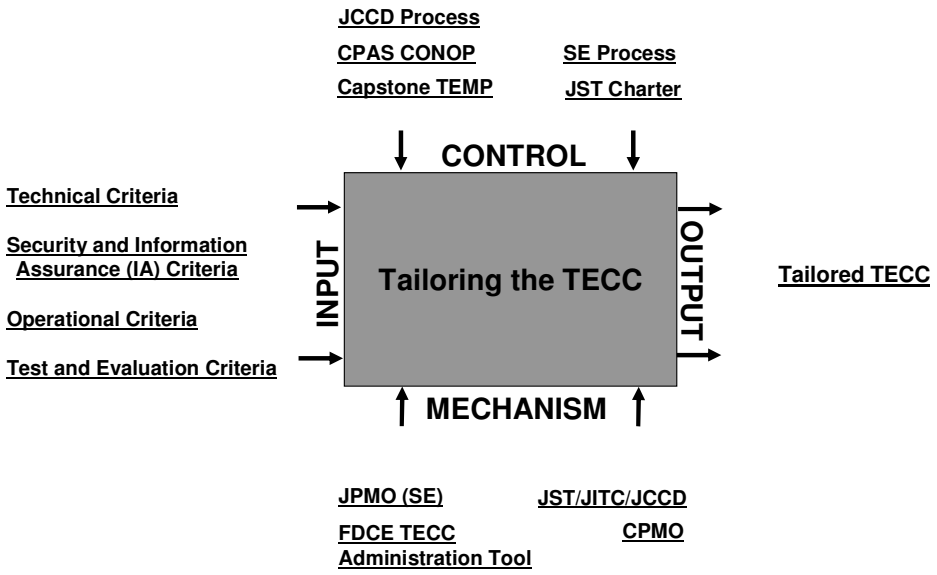

Figure 5: TECC Tailoring Function Model

Input to the TECC is an iterative four-step building process:

1) Technical Criteria: Establish standard systems engineering and specific performance parameters of the CM. These requirements are determined as part of the CDP engineering process requirements for a CM to operate in a SOA environment. These requirements typically pertain to most CMs.

2) Security and Information Assurance (IA) Criteria: Identify specific policy requirements for the CM (e.g., Net-Ready (NR), Information Assurance Level, etc.). These requirements are also fairly inclusive of the entire NECC CM family.

3) Operational Criteria: Identify specific Warfighter criteria. These criteria vary by CM but include performance requirements aligned to Mission Capability Packages (MCP), derived requirements generated by the systems engineering EMT development process, and those requirements associated with DOT_LPF-P issues.

4) Test and Evaluation Criteria: Identify specific T&E and other unique certification requirements. These include Measures of Effectiveness (MOEs), Measures of Suitability (MOSs), and Measures of Performance (MOPs). The Joint System Team membership determines these attributes through active participation in the CDP development and test planning processes.

Governed by program documentation and processes, the Materiel Provider, Warfighter, and TEC communities use the tailored FDCE TECC Administration Tool as the mechanism to examine and manage the tailored TECC for each CM to determine the appropriate level of developmental and operational testing (scope and activities) to mitigate risks. By employing a risk-based management framework, testing and certification processes are rapidly applied to a CM based upon its assessed maturity. These processes are illustrated in Figure 6 and are further described below.

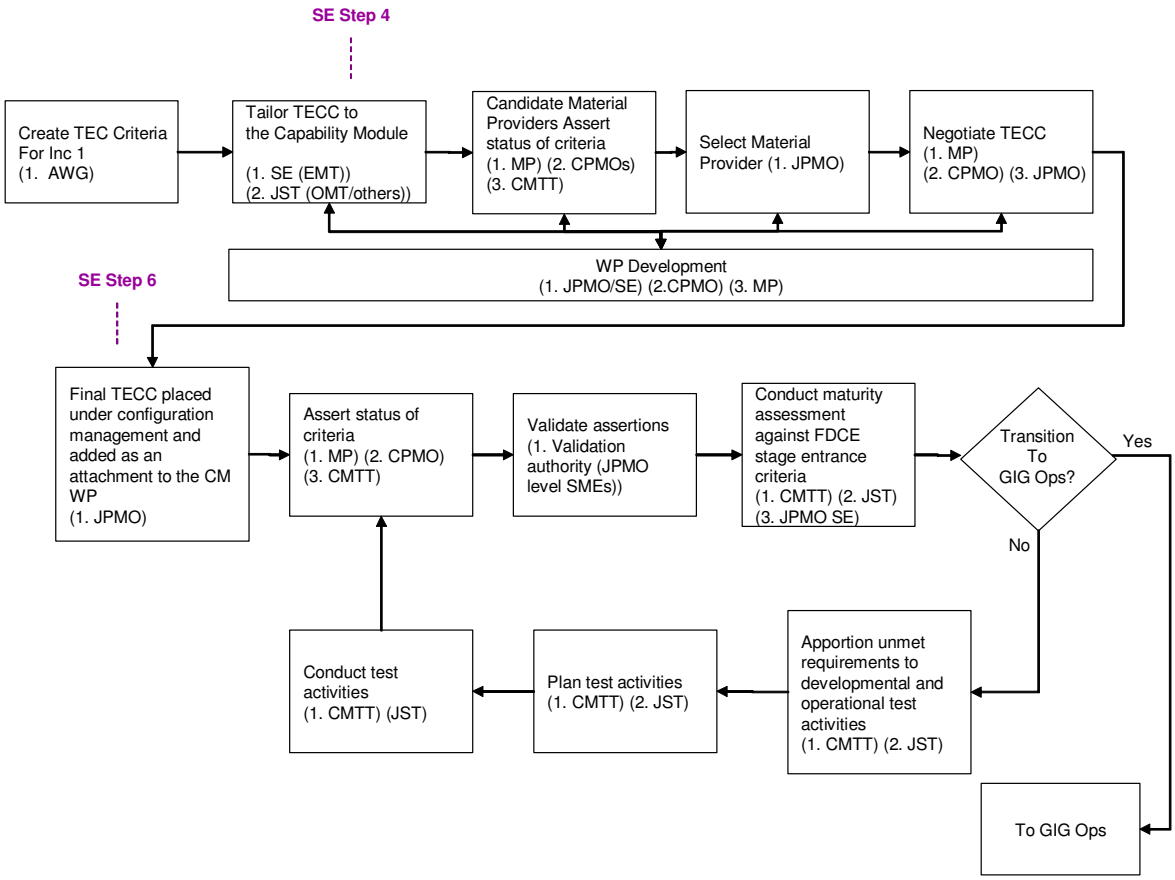

Figure 6: TECC Tailoring and Test Activities Process

A.2.3.1 Creating TECC and Tailoring the TECC to the CM

The FDCE TECC Administration Tool provides the ability to group criteria into profiles (see Figure 7). There are two types of profiles, mandatory and discretionary. A mandatory profile applies to all CMs independent of any other effort to categorize or "bin" a particular CM. The technical guidance profile provides a good example of a mandatory profile because it shapes the environment nearly all CMs must function in. The ability to de-select requirements during the

tailoring process does not exist in a mandatory profile. If, during the negotiation process, an exception to the criteria contained in a mandatory profile is provided for in the WP, the exception is noted during the TECC assertions process described in paragraph A.2.3.4.

A discretionary profile addresses all of the unique requirements that apply to a CM; this includes broad functional area requirements (e.g., all Shared Situational Awareness CMs must do abc) as well as CM-specific performance requirements (e.g., process xx targets in yy seconds).

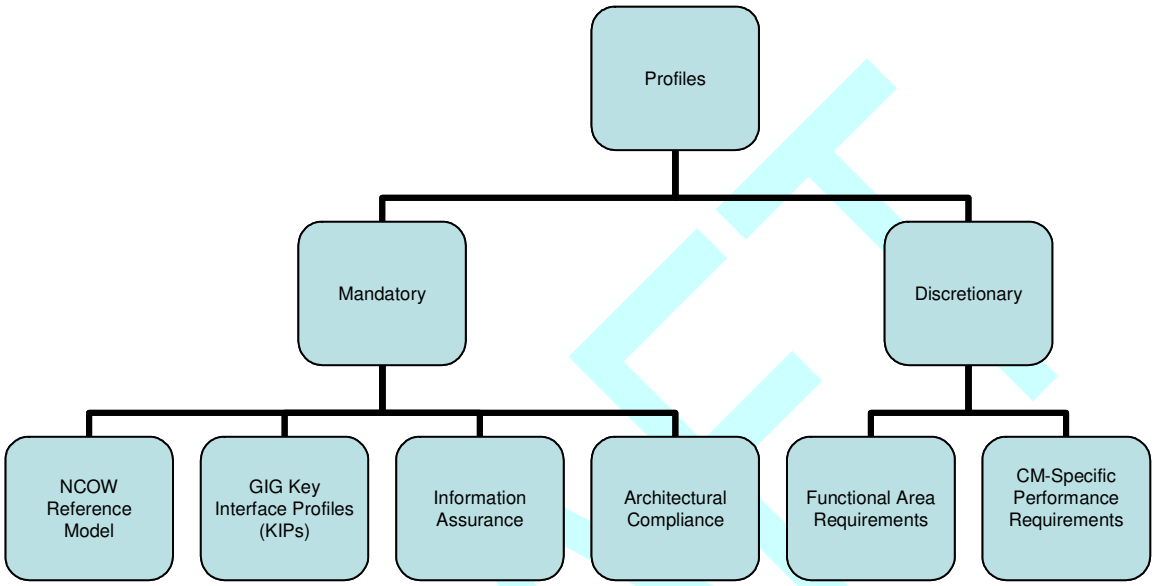

Figure 7: CM TECC Profiles

A.2.3.2 Using the TECC to Select a Materiel Provider

Once tailored for a CM, the TECC is made available to candidate materiel providers who work with their sponsoring CPMO to submit an assessment of capability maturity based upon asserting completion of the criteria contained in the tailored TECC. This facilitates the selection of the materiel provider by the JPMO. This process may be bypassed in cases where both the capability and the materiel provider are known and no competition or "best-of-breed" determination needs to be made. In either case, once the materiel provider has been selected, the tailored TECC are negotiated based upon the business aspects of the work package including cost, schedule, and the expected ability to meet performance parameters.

A.2.3.3 Configuration Management of the TECC

The finalized version of the tailored TECC is placed under configuration management and is attached to the CM's work package. This process maintains the integrity of the TECC and enables the iterative process of making assertions about the status of the TECC, validating those assertions, and conducting the test planning and execution processes.

A.2.3.4 TECC Assertions and Validation

The tailored TECC are placed into the FDCE in the associated CM's FDCE Workbook. The TECC are grouped in the display by the appropriate FDCE Stage in which the criteria must be satisfied. The display also shows the current status of the criteria contained in the tailored

DRAFT

TECC. The materiel provider, CPMO, and CMTT members review each of the criteria and make assertions on their status. Possible assertions on the CM's state of readiness include:

1) Met: The requirements of this criterion are fully satisfied.
2) Not Applicable: The requirements of this criterion do not apply because of an exception allowed for in the work package.
3) Deferred: This criterion has been deferred based upon a decision by the JPMO. Criteria are likely to be deferred if they have failed test and do not currently meet program expectations of cost, schedule, and performance. Deferred requirements must still be satisfied by the materiel provider. A later build may accommodate criteria with this status.
4) Waived: This assertion follows negotiation with the JPMO SE and JST, specifically the JCCD, and is used to advance a criterion that meets the "80%" solution. Waiving a requirement accepts the condition of the criterion "as is." Criteria are likely to be waived if they have failed test by not meeting threshold requirements, are not critical to the development of the CM, and do not meet program expectations of cost, schedule, and performance. For example, a threshold requirement may be "do 50." Test results show that the CM can "do 45." Technically a failure, the results of the test force the CM into a programmatic tradespace to conduct additional testing (e.g., re-test), defer the requirement, or waive the requirement. Unlike a deferred requirement, a waiver does not require the materiel provider to improve the condition of the CM to satisfy the requirement.

The FDCE TECC Administration Tool provides the means to attach hyperlinks to artifacts that support the assertion. Amplifying comments can also be made.

Once an assertion is entered by the materiel provider, the FDCE TECC Administration Tool alerts the appropriate validation authority that an assertion has been made and requires a responsive action. A matrix of assertion and validation authorities is shown in Figure 8, below this subsection. The validation authority examines the assertion, associated evidence, and any comments made by CPMO and either accepts or rejects the assertion. The validation authority may also include comments concerning the validation decision. The interaction between the assertion and the validation authorities is captured in the FDCE TECC Administration Tool and contributes to the history of the CM's development while also providing the most current information for others in the program.

Assertions are also made based upon a CM's test status. The FDCE TECC Administration Tool makes these assertions automatically, thus freeing the event planner from the need to manually update each criterion. Using the FDCE to plan a test event (e.g., CPE) enables the planner to apportion any number of criteria to that event. Upon selecting the criteria, the status of the criteria is automatically changed to "planned." Once the CPE plan is approved, the status of the criteria apportioned to that event is automatically changed to reflect "scheduled". At the conclusion of the CPE the status changes to "tested" and so on throughout the test process. The validation authority is notified of the status assertion and acknowledges the status of all the apportioned criteria with a single action. In this way, the validation authority is always kept apprised of the current test status of a CM. Assertions based on a CM's status include:

1) Untested: Criteria that have never been apportioned to a test event.

2) Planned: Criteria that are apportioned to a test event that does not yet have an approved test plan.

3) Scheduled: Criteria that are assigned to an event that has an approved test plan including a scheduled start date.

4) Tested: Criteria that are assigned to an event which has begun, but the outcome of which has not yet been reported.

5) Assessed: Criteria that have completed test and the outcome is reported.

6) Re-test: Criteria that are currently assigned to a test, but have been tested previously. These criteria will normally be re-tested within the cost and schedule parameters of the original work package.

TECC Assertion and Validation Authorities

Validation Area	Development	Developmental Piloting	Operational Piloting
Technical Criteria	CPMO / CMTT	CPMO / JPMO (SE)/ JST	CMTT (OT) / ATEC
Security and IA Criteria	CPMO (NR-KPP) (IA) / JITC/JPMO (NR-KPP) (IA)	CPMO (NR-KPP) (IA) / JITC/JPMO (NR-KPP) (IA)	CMTT (OT) / ATEC
Operational Criteria	CPMO / CMTT	CPMO / CMTT	CMTT (OT) / ATEC
Test and Evaluation Criteria	CPMO / CMTT	CMTT / JST	CMTT (OT) / ATEC

Assert / Validate

Figure 8: TECC Assertion and Validation Authorities

A.2.3.5 Conduct Maturity Assessment Against FDCE Stage Entrance Criteria

In some cases, adopted capabilities will satisfy the entrance criteria for an advanced stage of development like the Operational Piloting stage. In other cases, the capability will need to mature through each stage of the FDCE. The iterative process of reviewing the maturity of a CM and apportioning unmet TECC criteria to phases of developmental or operational test continues until the CM is assessed as meeting all requirements for transition to Global Information Grid operations (GIG Ops).

A.2.3.6 Apportion Unmet Requirements to Developmental and Operational Test Activities

Apportioning unmet requirements/criteria to the appropriate phase of test will, in most cases, occur as soon as the initial assertions are validated by the appropriate authority. The initial

apportionment influences the test strategy for the Test and Evaluation Master Plan (TEMP) Annex. Apportionment is an iterative activity that takes place upon analysis of test results and the assertion-validation process. The apportionment process recurs until the CM is certified for transition to GIG Ops. The apportionment process requires the CMTT to analyze the unmet requirements and consider such factors as:

1) Design of the CM. The success of some criteria may be predicated on the successful development of other criteria. The CM may also be dependent on the maturity of supporting CMs.
2) Priorities of the criteria (CTP, early build v. later build, etc.)
3) Alignment of criteria to FDCE stage of maturity

The FDCE TECC Administration Tool provides the appropriate views and reports to facilitate test planning of unmet criteria.

A.2.3.7 Plan Piloting Activities

As discussed in paragraph A.2.1, NECC uses piloting to providing a framework where technology demonstrations, experimentation, and T&E can be conducted in a realistic SOA environment. Piloting activities are planned in the FDCE environment. This provides a comprehensive view of all CMs under assessment. The FDCE environment also provides the means of developing the piloting event collaboratively. This accelerates the staffing process by allowing all the key stakeholders to contribute to the plan in a distributed, asynchronous manner. Milestone activities may be established with associated due dates. Templates for all piloting documentation are being developed so that they are available for completion on-line.

A.2.3.8 Conduct Piloting Activities

The checklists for piloting event readiness reviews are also completed on-line. Post-event analysis is conducted and the applicable event reports are completed using the on-line templates provided in the FDCE. The analyzed results of piloting activities are used to make assertions of unmet requirements and the iterative process is repeated until the CM is certified as ready to transition to GIG operations.

A.2.4 Certification Entrance Criteria

In order to gain entrance to a particular certification stage, a CM needs only to pass the criteria for that stage. Although the CM does not have to physically pass through all previous stages, it does have to provide evidence that all criteria for prior stages have been met.

In the event that a CM fails to be promoted, evaluators will spell out the reasons for failure and return the CM to the responsible CPMO and to the Materiel Provider for correction and re-submission.

The main certification categories are:

1) Net-Ready Key Performance Parameters (NR-KPPs)
2) Mission Capabilities
3) Performance

DRAFT

Each of these main categories has sub-categories and elements that further enumerate the important certification criteria for a particular stage. Typical criteria include the following:

1) Registration: Defines the purpose of the capability module. It identifies Governmental organization affiliation and sponsorship.
2) Security: Certifies that services are compliant with the core enterprise security model.
3) Configuration Management: Certifies that services conform to the configuration management processes associated with the maturity of the stage.
4) Training: Certifies that requisite training materials for a CM have been provided.
5) Enterprise Service Management (ESM) Enabled: Certifies that services are compliant with the reporting requirements of the NCES-provided enterprise service management service. Examples of such reporting requirements include:
    a) Availability Guarantees: Certifies that services have established minimum availability thresholds and are able to meet them.
    b) Response Time Guarantees: Certifies that services have established minimum performance thresholds on the response time of their service and that they are able to meet them.
    c) Reliability/Survivability Guarantees: Certifies that services have established minimum reliability/survivability thresholds and are able to meet them.
6) NETOPS Ready: Certifies that services have provided mechanisms for supporting enterprise Network Operations (NETOPS) activities.
7) On-Line Help: Certifies that services provide on line help (either built in or via a help desk).
8) Lifecycle Commitments: Certifies that a service provider has committed to keep the service operational for a specified period of time.

For the Development Stage, it is important to have as low a "barrier to entry" as possible. Consequently, for this stage, entrance criteria are primarily limited to registration information that identifies the following:

1) High-level description of the CM
2) Governmental organization affiliation and sponsorship
3) CDP and CDD linkages (for requirements traceability)
4) Mission Area (e.g., Adaptive Planning, Force Protection, Situational Awareness, etc.)
5) Endpoint/Link to capability (if known)
6) Link to NCES Service Registry entry

A.2.5 FDCE Stage Governance

The following sections describe the business rules that govern the promotion of CMs from one FDCE stage to the next and finally, from the Operational Piloting stage to Operations (i.e., Limited Fielding). Prior to entering the FDCE the CM Developer performs a "maturity" assessment. The NECC Maturity Assessment Tool (NMAT) spreadsheet task must be completed

and made available via the FDCE. If a CM Developer believes their capability is ready to enter the process at a more mature stage of the FDCE based on the NMAT assessment, the CM Developer & controlling CPMO then request that the JPMO Systems Engineering Branch perform an evaluation of the entire set of artifacts (per the Developmental Piloting Checklist) including the Risk Assessment, Systems Engineering artifacts, test artifacts, IA status, etc. Typically, the NMAT results will find that the CM is not ready for advancement into Developmental Piloting or Operational Piloting. Instead, NMAT will support developers by indicating what areas they should concentrate their development efforts on to reduce risk.

A.2.5.1 Development to Developmental Piloting

The Development Stage is the first CM entry stage of maturity for capability development and certification. This stage focuses on initial CM development, debugging, and technical exploration of capabilities.

Entrance criteria for this stage are set as low as possible to minimize the barriers for participation. Development Stage entrance criteria include completing internal CM testing against GIG and non-GIG networks. This stage tests the CM against the specifications dictated in the CM Work Package. Depending upon the CM's maturity, various User Free Play (UFP) events will be conducted so that operational users can assess CMs and provide early feedback on operational utility.

Through all FDCE stages, Material Providers (w/CPMO participation as needed) make assertions against the TECC in the FDCE. That is, the FDCE provides the ability for CM Developers to assert whether or not their CM meets the criteria established in its tailored TECC, in order to advance through the stages. Developers must provide evidence (i.e. test results) to support their position (assertions).

For the Development Stage, the JPMO Systems Engineering Branch has the responsibility for validating the evidence provided by the developer. Systems Engineering ensures that all the correct standards for the CM were addressed in the assertions prior to this validation.

An assertion has been validated when the evidence offered for the assertion is accepted by the validating authority. The validating authority for the FDCE Development Stage is the NECC Chief Engineer. The Chief Engineer tasks the NECC Systems Engineering Branch to conduct a review of all the applicable CM artifacts with a recommendation that will support his/her decision. Validated requirements, with the exception of those requirements specifically identified by the OT community, require no further testing. This allows the developer and test community to focus future CPAS on requirements that have not been validated.

Once a CM's assertions are approved (Development Stage artifacts posted in the FDCE and verified as acceptable evidence) the developer is notified by the JPMO that the CM is ready to proceed to Developmental Piloting If a CM is determined <u>not</u> to be ready to proceed to Developmental Piloting, the CM Developer is provided a list of shortfalls. The CM Developer is responsible for rectifying those shortfalls as needed and then re-conduct/review the risk assessment as needed. In some cases, a CPAS event (i.e., CPE) may be required to rectify a shortfall.

DRAFT

Figure 9 provides a high-level summary of the FDCE stages and the decision makers responsible for promotion to the next stage. Figure 10 depicts the process flow for promotion from the Development Stage to the Developmental Piloting Stage. Table 3 comprises a notional checklist of the applicable TEC Criteria a CM must meet in order to be promoted from the Development Stage to the Developmental Piloting Stage.

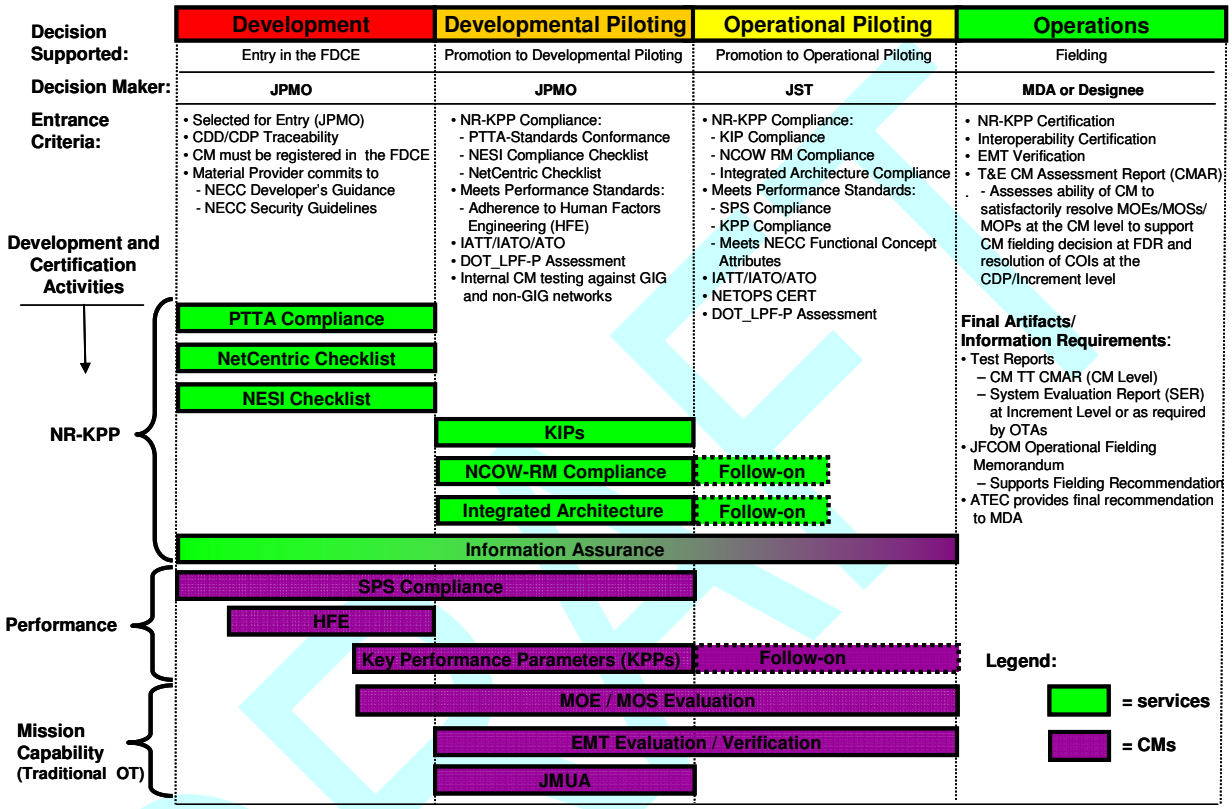

Figure 9: FDCE Stage Entrance Criteria for a CM and the Decision Makers

DRAFT

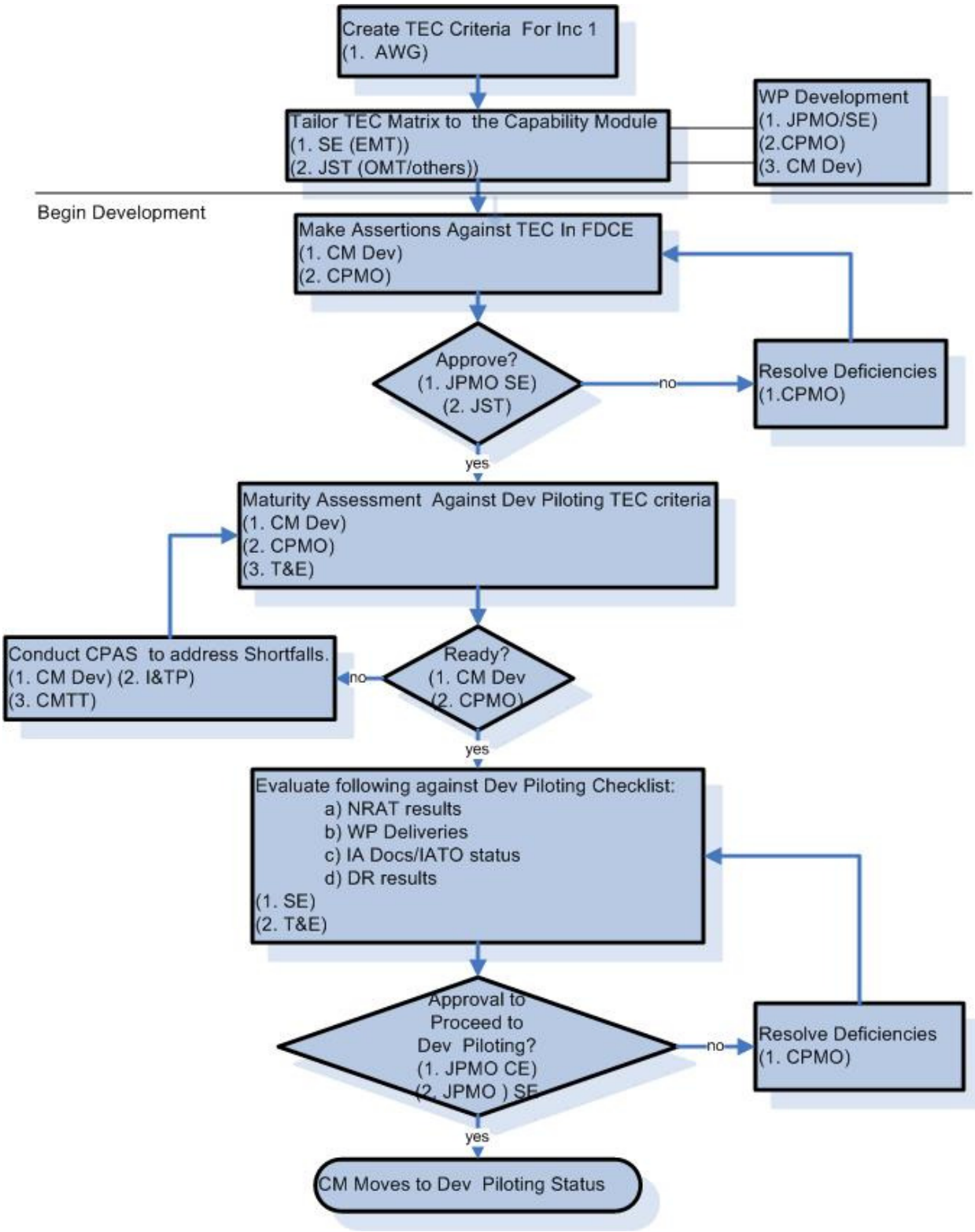

Figure 10: Promotion from Development to Developmental Piloting

Table 3: Notional Criteria for CM Promotion from Development to Developmental Piloting

TECHNICAL CRITERIA (JPMO & CPMO)			
Data Services			
1)	SOAP 1.1	Y / N	
2)	WSDL 1.1	Y / N	
Thick Clients			
3)	MS Windows 2000 or later	Y / N	
Thin Clients			
4)	HTML 4.01	Y / N	
5)	No browser specific extensions	Y / N	
6)	Java 1.5 for any applets	Y / N	
7)	Flash version 7 or greater for any Flash-based applications	Y / N	
8)	IE 6.0 or higher, Mozilla Firefox 1.5 or higher	Y / N	
Schemas			
9)	XML Schemas for all XML documents	Y / N	
10)	Version XML Schema files separately from the XML components defined in those files	Y / N	
11)	Declare all named XML schema components within a namespace (all XML Schema documents shall have a target Namespace attribute on the schema element)	Y / N	
12)	Use XML Namespaces for versioning XML components. Define new version of XML components in a new XML namespace	Y / N	
13)	Use http://metadata.dod.mil/mdr/ns as the prefix for XML namespace names and devise a scheme for the user-defined portion of the namespace name that supports the CM process	Y / N	
Systems Engineering/Work Package Deliverables			
14)	Evidence for items 1-25 of the Tech guidance have been examined and are acceptable by T&E. Any non-conformance issues are adequately documented in the CM Developers compliance roadmap schedule.	Y/N	
15)	Architecture Complete and Approved?	Y/N	
16)	Web Service Specifications Provided and Approved?	Y/N	
17)	IATO or IATT complete and approved?	Y/N	
18)	CPMO/CM Developer Risk Assessment and Status updated (for Developmental Piloting). This is the CM's monthly risk assessment report. This document proves that the CPMO and/or developer is performing Risk identification & mitigation activities for Performance, Cost, & Schedule as a part of the development process.	Y/N	
19)	Hosting and Sustainment Documentation is Complete and Approved?	Y/N	
20)	FDCE Registration is Complete?	Y/N	
21)	Software is Available for use Online (NIPRNet or SIPRNet)	Y/N	

22)	Design Review successfully completed?	Y/N	
SECURITY AND INFORMATION ASSURANCE CRITERIA (DAA & FSO)			
23)	STIG/SRR process compliance	Y / N	
24)	SSL technology for information that has sensitivity to release outside DoD	Y / N	
25)	Service-Service communication protected with SSL when transmitted outside of the network enclave protecting the individual service	Y / N	
26)	Authentication mechanism preference in order: CAC, DoD soft certificates, ECA certificates, JITC certificates, username/password. In all cases, authentication protected by SSL sessions (NIPRNet)	Y / N	
27)	Server certificates issued by PKI Program Office, LRA, or JITC (NIPRNet)	Y / N	
28)	Server-Server communications encrypted with authenticated SSL using proper certificates when communicated outside of the network enclave protecting the servers (NIPRNet)	Y / N	
29)	Authentication mechanism preference in order: DoD soft certificates, username/password (SIPRNet)	Y / N	
30)	Servers use server certificates issued by the PKI Program Office or LRA (SIPRNet)	Y / N	
31)	Information transmitted outside of network enclave encrypted using SSL	Y / N	
OPERATIONAL CRITERIA (JFCOM)			
36.	Training Packages Reviewed	Y/ N	
37.	Warfighter Input/Lessons Learned captured (UFP)	Y/ N	
38.		Y/ N	
39.		Y/ N	
NCES Services			
40.	NCES Service Discovery	Y / N	
41.	NCES Metadata Registry	Y / N	
TEST AND EVALUATION CRITERIA (ATEC and Supporting OTAs)			
42.	CM TT confirms adequacy of SE documentation	Y/N	
43.	All required CM documents reside in the FDCE	Y/N	
44.	CM Detail Test Plans for Dev Pilot CPAS events approved	Y/N	
45.	CM Test Resources/Tools for Dev Piloting stage ready	Y/N	
46.	CM T&E Metrics/Earned Value requirements understood	Y/N	
47.	CM TT recommends advancement to Dev Piloting stage	Y/N	
48.	JST briefed on CM Status and Dev Piloting test plan	Y/N	
49.	CM Tailored Matrix – Criteria Demonstrated to Date	TBD	

DRAFT

A.2.5.2 Developmental Piloting to Operational Piloting

The Developmental Piloting Stage is the second stage of maturity for capability module development and certification. The primary purpose of this stage is to test and certify the net-ready status of the capability, receive an IATO (or IATT) for operations on the GIG and reduce operational risk. At this stage, operational users can begin to assess CMs to provide early feedback on operational utility. Entrance criteria for this stage focus on achieving a sufficient level of technical stability and standards conformance. Developmental Piloting Stage entrance criteria include completing internal CM testing against GIG and non-GIG networks. Meaningful Warfighter assessment requires sufficient service description, usage, and instruction (Training) to support and encourage Warfighter participation, questions, and feedback. Developmental Piloting Stage exit criteria (i.e., Operational Piloting Stage entry criteria) include completing interoperability and compatibility testing against other systems and applications with which the CM exchanges information on GIG and non-GIG networks. This stage should test the application/CM with other CMs/applications/systems.

While the process to manage the Developmental Piloting stage works like Development to Developmental Piloting, the roles and responsibilities do change. The JST has approval authority to promote a CM to Operational Piloting. The Operational Piloting Checklist is an expanded version of Developmental Piloting checklist and includes items like UFP/CPE results and compliance with a more comprehensive set of standards and specifications.

Figure 11 depicts the decision-making and process flow for promoting a CM from the Developmental Piloting Stage to the Operational Piloting Stage. Table 4 is a notional checklist of the applicable TEC Criteria a CM must meet in order to be promoted from the Developmental Piloting Stage to the Operational Piloting Stage.

DRAFT

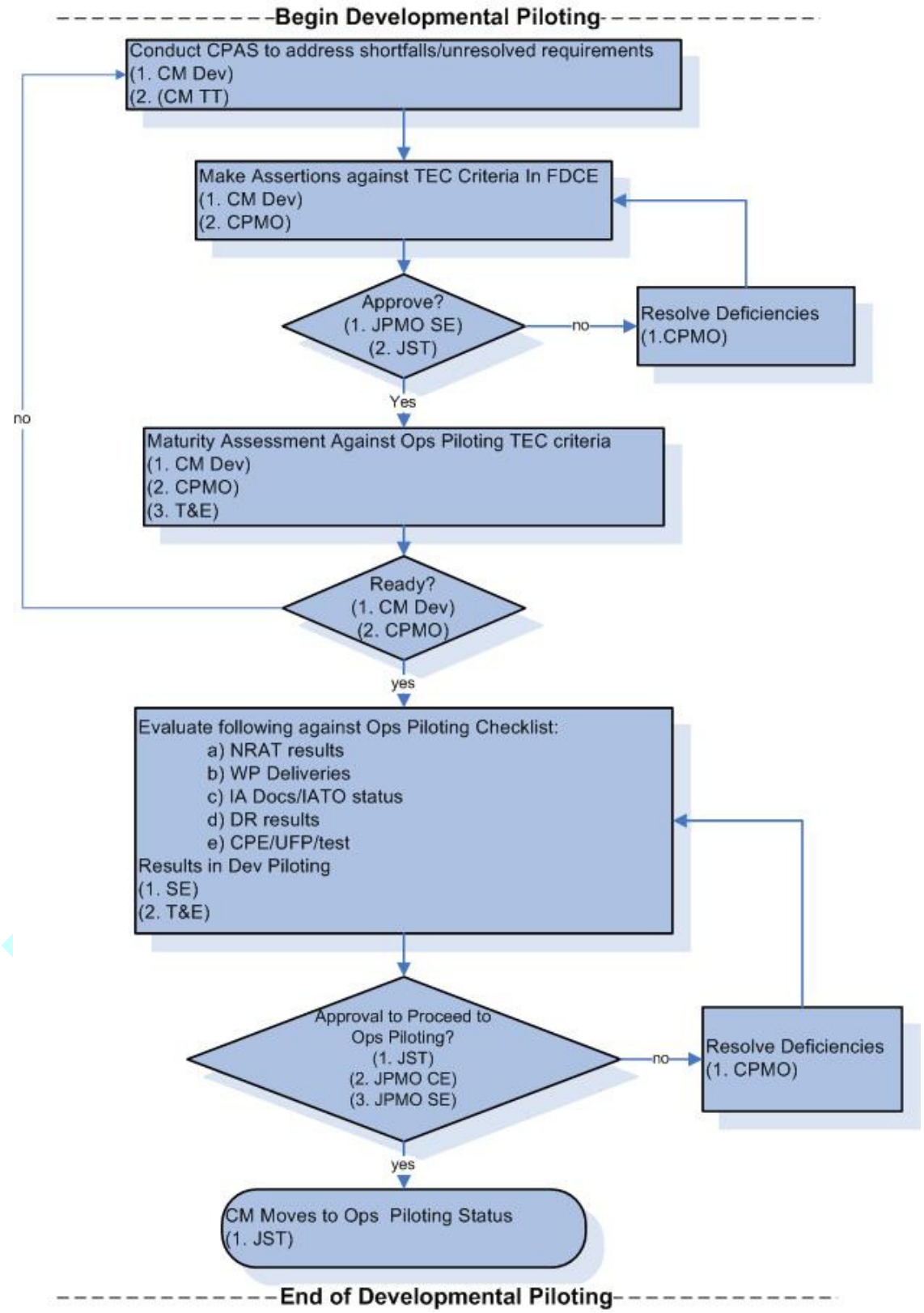

Figure 11: Promotion from Developmental Piloting to Operational Piloting

Table 4: Notional Criteria for CM Promotion from Developmental Piloting to Operational Piloting

Data Services			
1)	SOAP 1.1 (recheck only if any major changes have incurred from Dev)	Y / N	
2)	WSDL 1.1 (recheck only if any major changes have incurred from Dev)	Y / N	
3)	WS-Management	Y / N	
4)	WS-Addressing for SOAP header in accordance w/ WS-Management 2.1	Y / N	
5)	Use WS-Addressing in the SOAP header to specify a unique Resource URI for each object managed by the data service in accordance with WS-Management 2.1. The resource URI must be a valid URI and Y / N uniquely identify the resource within the scope of the service	Y / N	
6)	Expose read operations (the "Get" action on their resources using the WS-Transfer protocol in accordance with WS-Management section 4.4	Y / N	
7)	Expose a query interface to the resources using the Xpath and WS-Enumeration in accordance with WS-Management section 5.1	Y / N	
8)	Create, Update and Delete operations. If these operations are provided by a service they shall use the WS-Transfer protocol in accordance with WS-Management sections 4.5, 4.6 and 4.7.	Y / N	
9)	If the data service exposes an asynchronous public interface, it shall use the WS-Eventing in accordance with WS-Management section 7.1.	Y / N	
10)	Support a subscription filter mechanism using Xpath for every asynchronous interface in accordance with WS-Management section 7.2.2	Y / N	
11)	Support the "heartbeat" function for every asynchronous interface in accordance with WS-Management section 7.2.5	Y / N	
Presentation Services			
12)	Expose data suitable for rendering on a map, using WMS 1.1.1 specification	Y / N	
13)	Support the query subset of SLD for every WMS service	Y / N	
14)	Support PNG and JPEG image formats for every WMS service	Y / N	
15)	Expose geospatial feature data using WFS 1.1 specification	Y / N	
Thick Clients			
16)	MS Windows 2000 or later (recheck only if any major changes have incurred from Dev)	Y / N	
Thin Clients			
17)	HTML 4.01 (recheck only if any major changes have incurred from Dev)	Y / N	
18)	No browser specific extensions (recheck only if any major changes have incurred from Dev)	Y / N	
19)	Java 1.5 for any applets (recheck only if any major changes have incurred from Dev)	Y / N	
20)	Flash version 7 or greater for any Flash-based applications (recheck only if any major changes have incurred from Dev)	Y / N	

DRAFT

21)	IE 6.0 or higher, Mozilla Firefox 1.5 or higher (recheck only if any major changes have incurred from Dev)	Y / N	
Schemas			
22)	XML Schemas for all XML documents (recheck only if any major changes have incurred from Dev)	Y / N	
23)	Version XML Schema files separately from the XML components defined in those files (recheck only if any major changes have incurred from Dev)	Y / N	
24)	Declare all named XML schema components within a namespace (all XML Schema documents shall have a targetNamespace attribute on the schema element) (recheck only if any major changes have incurred from Dev)	Y / N	
25)	Use XML Namespaces for versioning XML components. Define new version of XML components in a new XML namespace (recheck only if any major changes have incurred from Dev)	Y / N	
26)	Use http://metadata.dod.mil/mdr/ns as the prefix for XML namespace names and devise a scheme for the user-defined portion of the namespace name that supports the CM process (recheck only if any major changes have incurred from Dev)	Y / N	
Data Standards			
27)	DDMS Version 1.3	Y / N	
28)	Enterprise Discovery	Y / N	
29)	Create DDMS conformant XML Document (metacard)	Y / N	
30)	Store metacard in location that is accessible to the NCES Federated Search Tool	Y / N	
31)	Describe information resource at the lowest classification level	Y / N	
32)	GML 3.1.1 Used to represent geo-spatial information	Y / N	
33)	IC-ISM Version 2.0	Y / N	
34)	Associating security related metadata with XML elements in documents, web-service transactions or data streams	Y / N	
35)	Date/Time Format (ISO 8601 W3C Profile)	Y / N	
36)	All Date/Time encoded in ISO 8601	Y / N	
IA Guidance			
37)	STIF/SRR process compliance (recheck only if any major changes have incurred from Dev)	Y / N	
38)	SSL technology for information that has sensitivity to release outside DoD	Y / N	
39)	Service-Service communication protected with SSL when transmitted outside of the network enclave protecting the individual service (recheck only if any major changes have incurred from Dev)	Y / N	
40)	RBAC/ABAC (objective)	Y / N	

DRAFT

41)	Authentication mechanism preference in order: CAC, DoD soft certificates, ECA certificates, JITC certificates, username/password. In all cases, authentication protected by SSL sessions (NIRPNET) (recheck only if any major changes have incurred from Dev)	Y / N	
42)	Server certificates issued by PKI Program Office, LRA, or JITC (NIPRNet) (recheck only if any major changes have incurred from Dev)	Y / N	
43)	Server-Server communications encrypted with authenticated SSL using proper certificates when communicated outside of the network enclave protecting the servers (NIPRNet) (recheck only if any major changes have incurred from Dev)	Y / N	
44)	Authentication mechanism preference in order: DoD soft certificates, username/password (SIPRNet) (recheck only if any major changes have incurred from Dev)	Y / N	
45)	Servers use server certificates issued by the PKI Program Office or LRA (SIPRNet) (recheck only if any major changes have incurred from Dev)	Y / N	
46)	Information transmitted outside of network enclave encrypted using SSL (recheck only if any major changes have incurred from Dev)	Y / N	
NCES Services			
47)	NCES Security	Y / N	
48)	NCES Service Discovery (recheck only if any major changes have incurred from Dev)	Y / N	
49)	NCES Metadata Registry (recheck only if any major changes have incurred from Dev)	Y / N	
50)	NCES Federated Search	Y / N	
Systems Engineering/Work Package Deliverables			
1)	Evidence for items 1-51 (listed above) of the Tech guidance have been examined (as applicable) and are acceptable by T&E. Any non-conformance issues are adequately documented in the CM Developers compliance roadmap schedule.	Y/N	
2)	Architecture (if updated/modified as a result of Dev piloting) Complete and Approved?	Y/N	
3)	Web Service Specifications Provided and Approved? (These should be the same WSS that are under test!)	Y/N	
4)	Capability Package (CP) with all components required for the CM services(s) is complete.	Y/N	
5)	CPMO/CM Developer Risk Assessment and Status updated (for Developmental Piloting). This is the CM's monthly risk assessment report. This document proves that the CPMO and/or developer is performing risk identification & mitigation activities for Performance, Cost, & Schedule as a part of the development process.	Y/N	
6)	Metrics deliverable is up to date (for Operational Piloting).	Y/N	
7)	Any updates, if required, for the service on the FDCE have been completed?	Y/N	
8)	IATO or ATO complete for the version under test. DIACAP package is uploaded and has been reviewed and approved. (CPMO IA SME should be providing this assertion.)	Y/N	

DRAFT

9) SLA Assessment is complete and approved. Performance should meet the minimum specified in the Work Package SLA.	Y/N	
10) Test Documentation- Any test documentation being used to support assertions must be posted and approved.	Y/N	
11) Training guides and Plans must be submitted and approved.	Y/N	
12) Generated operational use cases and threads must be submitted and approved.	Y/N	
13) Hosting and Sustainment documentation should be updated as needed. Note: CPMOs should be updating their hosting and sustainment documentation to address IA related requirements during the Operational Piloting Phase.	Y/N	
14) Software is Available for use Online (NIPRNet or SIPRNet)	Y/N	
15) All scheduled developmental piloting UFPs completed and documentation uploaded and approved. UFP survey results meet the goals and objectives of the UFP announcement.	Y/N	
16) All scheduled developmental piloting CPEs completed and documentation uploaded and approved. CPE Assessment Report results meet threshold or better of R&P matrix.	Y/N	
17) DT Testing complete. Problem Reports have been adjudicated and resolved.	Y/N	
18) Early Operational Assessments (EOA). Any EOA assessment results have been reviewed and adjudicated.	Y/N	

A.2.5.3 Operational Piloting to Operations (NetOps)

The Operational Piloting stage is the final stage of maturity prior to a CM's operational deployment. The purpose of this stage is to evaluate and certify the operational utility and readiness of the CM to support the Warfighter capability. CMs enter operation piloting for one of three reasons:

1) To ensure readiness for Operation Testing and subsequent fielding
2) To support Integration and Technology Piloting activities
3) To establish a substantiation of a fielded CM (MDA Approved) in the FDCE in order to support integration activities required of developing CMs

Those CMs that are ready for Operational Testing and eventual fielding will undergo an Operational Test Readiness Review (OTRR) that will be chaired by the JST. Those CMs that are entering Operational Piloting to solely support I&TP activities will only need to be certified by the JPMO. CPAS elements during the Operational Piloting Stage evaluate and certify the operational utility of CMs. At this stage, CMs have matured sufficiently to participate in operationally representative events and have addressed all security accreditation requirements. Entrance criteria for this stage include net-ready certification, IATO (or IATT) and sponsorship from an operational community.

DRAFT

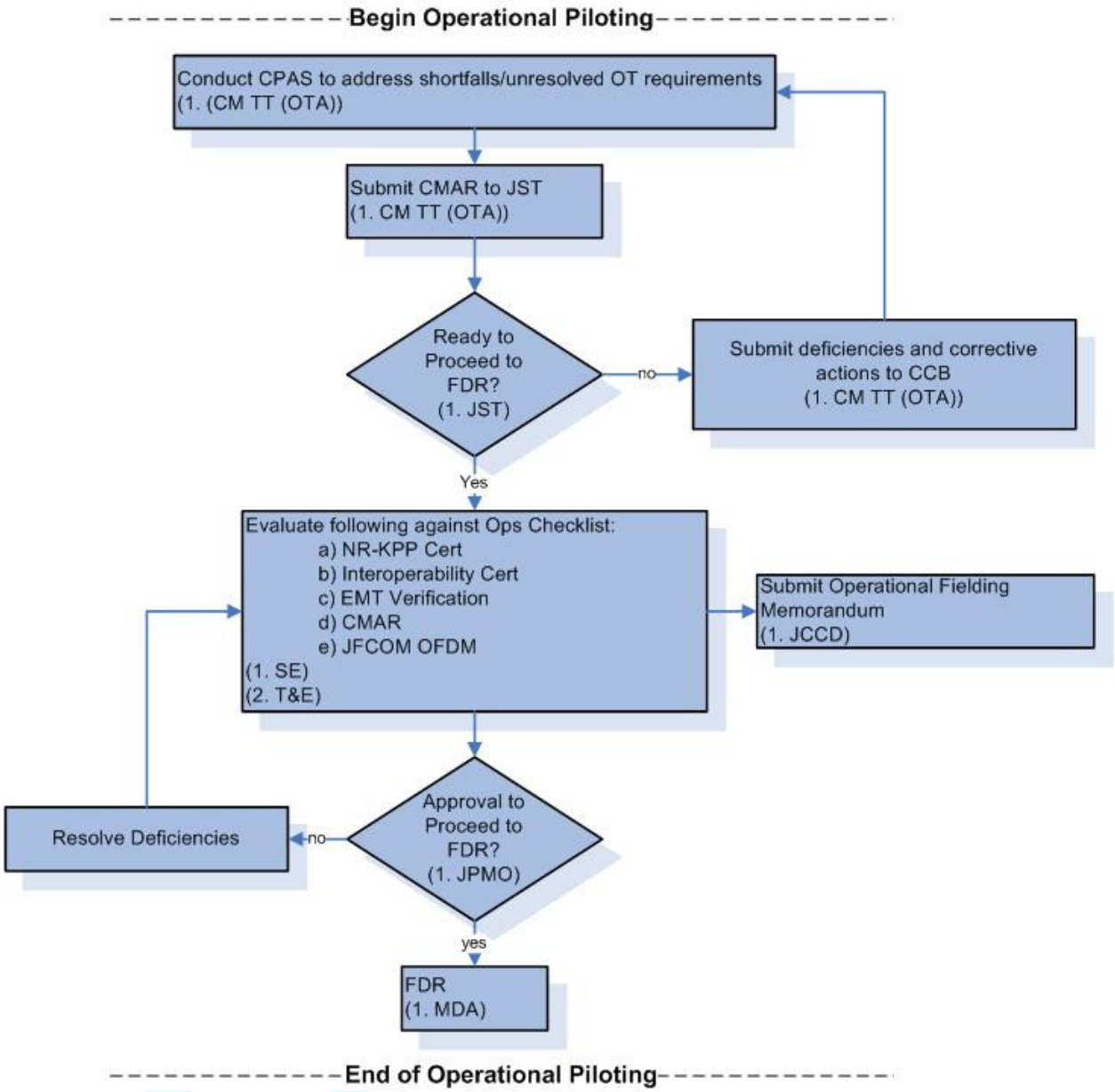

Figure 12: Promotion from Operational Piloting to Limited Fielding

A.2.6 FDCE Portal Functionality

The FDCE Prototype Portal provides support for the following functions:

1) Capability Module Definition
2) CM Selection Process (includes JPMO publishing of a requirement, CPMO response with tailored TEC criteria, evaluation of responses, and risk assessments at various junctures)
3) Work Package Development
4) CM Maturity Assessment (JITC approach) – aka NECC Maturity Assessment Tool (NMAT)

5) Tailoring of the TEC Criteria for a CM and refinement of that tailoring as the CM matures (as required)
6) Allocation to proposed CPAS events to serve as data sources for the TEC Community
7) CPAS Tracking, Planning, and Execution (to include Warfighter participation and evaluation)
8) TEMP Annex Development (Test Plans for DT and OT)
9) Automation Support for Capability Provisioning Event (CPE) / CM Test Planning and Reporting
10) Maintenance of the TEC Criteria List and tailoring support (to include a Tools Matrix that delineates available tools to test specified TEC criteria)
11) Role-specific user views (e.g., IA Page, Tester Page, Warfighter page)

A.3 FDCE Stakeholders - Roles and Responsibilities

Various DoD communities have different roles and responsibilities for interacting with the FDCE. The following sections outline the user communities, their community roles, and related FDCE tasks.

There are three primary stakeholders outside of the JPMO's Systems Engineering team who play a critical role in the maturation of CMs within the FDCE. They are: 1) Materiel Providers, 2) Testers, Evaluators, and Certifiers, and 3) Warfighters, to include the DOT_LPF-P role (to supply requirements and policy guidance to the NECC community). They are all essential to the development, T&E, and review/approval of any capability being managed by the NECC JPMO.

A.3.1 Materiel Providers

The Material Provider / Sustainment Community participates in CPAS by developing, maturing, operating, and sustaining enterprise-operated CMs. Materiel Provider organizations include the major C2 system commands and agencies (DISA, ESC, MCSC, SPAWAR, and CELCMC) as well as other Materiel Providers such as NGA, DIA, and NSA. COCOMs can also be Materiel Providers and support CM maturation.

A.3.1.1 What Is a Materiel Provider?

Materiel Providers can be government or non-government entities. A Materiel Provider is any prospective or current "Service" provider who is willing to conform to the architectural, data, information technology, and security standards defined for NECC and published on the Defense (DoD) Information Technology Standards Registry (DISR). These standards are intended to ensure that Materiel Providers produce capabilities that promote interoperability, reusability, and composability.

Examples of Materiel Provider include "data" providers, such as the Actionable Situational Awareness Pull (ASAP) Advanced Concept Technology Demonstration (ACTD). In this case, the Air Force Electronic Systems Command (ESC) commissioned its Engineering team (L-3 Com) to act as Materiel Provider to the DISA NECC program with the development of a new web services (net-centric) data access to data from the Integrated Broadcast Service (IBS). IBS provides National, Theater and Tactical Intelligence data pushed out in high volumes of

messages. ASAP, in conforming to the Net Centric Data Strategy and in compliance with the DISR standards produced a query or "user Pull" web service according to the net centric tenets. The web services produced were registered with the FDCE, were certified as standards-compliant (WSDL, SOAP, XML, Security), and consistent with other policies (i.e., naming conventions, SLA definition, etc.), and were published in the NECC Universal Description, Discovery, and Integration (UDDI) for user discovery of these new services.

Most Programs of Record migrating to net-centric standards will be Materiel Providers who provide access to data and other services (i.e. data fusion, visualization) that might benefit any number of users, and in particular the unanticipated user.

A.3.1.2 How Does One Become a Materiel Provider?

As noted briefly above, the process to become a Materiel Provider is facilitated by the FDCE which offers guidance and an automated set of tools that checks for compliance and guides the developer through the process required to be a recognized Materiel Provider. Specifically, the provider should register their capabilities with the FDCE. To do so, there are well established, documented procedures for publishing a Services Web Services Definition Language (WSDL), for documenting capabilities, for applying all appropriate web service standards (SOAP, WSDL, XML, SAML, etc.). By registering services (i.e., capabilities) and certifying their standards compliance, the Materiel Provider is also publishing the service for others to find and use. SLAs are established on-line in the final process required for becoming a good Materiel Provider, as this detailed agreement provides prospective users/consumers with the information they may need to "trust" this new service, to understand its maintenance and sustainment cycles and to ensure that the service supports the user needs regarding performance, reliability and operation.

A.3.1.3 Materiel Provider Roles and Responsibilities

The Materiel Provider must conform to the Net Centric web service standards defined within the NECC preliminary architecture document, as well as those published on the DISR website. These standards enforce that Materiel Providers apply Net Centric Enterprise Services available, and conform to good practice policies (such as those provided by the World Wide Web Consortium (W3C)).

In addition, Materiel Providers may be called upon to:

1) Develop, mature, operate, and sustain CMs.
2) Perform development, unit testing, and provide internal test certifications.
3) Collaborate with other Materiel Providers to facilitate the maturation of the CDP implementation approach.
4) Collaborate with other Materiel Providers to identify and share development resources.
5) Participate in or support in piloting events as required by NECC approved processes.

A.3.1.4 Oversight and Approval of Materiel Providers

Material Providers who are funded as DoD Materiel Providers are guided by OSD/NII net centric data strategy, DoD Discovery Metadata Standard (DDMS), and other guidance. A net-centric checklist is provided by OSD to ensure that DoD Materiel Providers conform to the established standards as defined under DISR.

DRAFT

A.3.1.5 Materiel Provider Business Processes when Interacting with the FDCE

The Business Process defined for FDCE participation is intentionally kept simple to ensure broadest participation and ease of use. These process steps are aligned with a flow that encourages Materiel Providers to publish their proposed CM (or Service) early in its development cycle, which facilitates increased opportunity to reuse existing/similar services already in development, and/or for prospective consumers of these services to help shape new capabilities for more than one purpose. The below list provides examples of the types of processes a Materiel Provider will be called on to support via the FDCE:

6) Register/publish new services
7) Update development status of services
8) Request service test, evaluation, and certification
9) Obtain service TEC status
10) Plan and execute pilot events to test and evaluate services
11) Support pilot events to test and evaluate services
12) Review pilot feedback on services
13) Negotiate/meet SLA requirements
14) Participate in the CMTT for applicable CMs.
15) Lead DT efforts on Component-assigned CMs and supports operational/integrated testing, when applicable.
16) As a member of the JST and CMTT, design, plan, program, coordinate, and execute a viable CM Integrated T&E program.
17) Assist in developing and tailoring the TEC criteria for assigned CMs.
18) Ensure CM work-related workspaces in the FDCE are complete and maintained for assigned CMs.
19) Coordinate CMTT actions with the material providers of the assigned CMs.
20) Assist in developing and maintaining NECC Integrated T&E documentation.
21) Coordinate the Integrated T&E strategy for each CM with the JST.
22) Facilitate CMTT actions to ensure appropriate CPAS documentation, and detailed developmental test plans and reports are accurate and submitted in the proper format and within required timelines.
23) Provide status report to the JST on progress/results of DT.
24) Participate in coordinating CPE events for assigned CMs.
25) Coordinate with the JPMO to fund IA validation/certification activities through the work packages.

DRAFT

A.3.2 TEC Community

The TEC Community includes policy makers, the test & evaluation communities, and the security accreditation community. This includes ASD(NII), DOT&E, AFOTEC, ATEC, COMOPTEVFOR, JITC, MCOTEA, ATEC, USSTRATCOM, USJFCOM, and JTF-GNO, as well as applicable security CAs and DAAs.

A.3.2.1 What Is a Tester/Evaluator/Certifier?

In the context of the NECC Program, certification is the process whereby a CM's technical requirements are tested/measured and evaluated against specified criteria and the results validated by the appropriate authoritative entity. In some areas, certification organizations are pre-determined (e.g., JITC for Interoperability Certification and DISA for NETOPS); in others, they are selected as was the case for the NECC IA Certification, where STRATCOM serves as the DAA. Developmental Testers are designated by the CM's CPMO to test NECC through its maturity cycle. Developmental Testers typically focus on lower level testing to validate that a CM meets required standards and performance specifications. Operational Testers typically assess/evaluate systems in an operationally representative environment using production representative systems with Warfighters operating the equipment.

A.3.2.2 How Does One Become a Tester/Evaluator/Certifier?

Developmental testing requirements are detailed in each service's Acquisition Program Management/Testing instructions/regulations. Acquisition Program Managers have overall responsibility for developmental testing and, depending on the service, the authority to select the DT test team for their programs. Operational Testing is a Title 10 of the US Code requirements. Further guidance is detailed in the DoD 5000.2 series documents and each of the service Acquisition Program Management/Testing instructions. Certifiers are generally identified by instruction/regulation; for example:

- DoD Instruction 4630.8 for NR KPP and Interoperability Certification
- DoDI 8500.2 for IA Certification

For the NECC Program, the JST defines the authoritative organizations/entities for testing and certifying (i.e., validating the results) of individual criteria in the TEC Criteria. Each organization/entity in turn then assigns specific individuals to serve as either formal testers or certifiers for specified TEC Criteria. Individual certifications will be valid for a one year period. FDCE Operations is responsible for maintaining the approved list of testers and certifiers.

A.3.2.3 Tester/Evaluator/Certifier Roles and Responsibilities

DoD Instruction 5000.2 series details specific requirements for operational testing and is expanded upon d in each of the Service's T&E instructions. Depending on the Service, DT requirements are outlined in the Major Command level instructions or in the Developmental Test Agency instructions. Specific certifications are discussed in specific instructions as mentioned above. Examples of specific responsibilities the TEC Community would perform via the FDCE include the following:

26) Establish and apply the (Tailored) TEC Criteria for CMs as they go through the certification processes

27) Observe Materiel Provider conducted CM testing events

28) Validate results of Materiel Provider testing

29) As necessary, independently test and evaluate CMs to ensure they meet certification requirements

30) Review CMs to ensure they meet security/IA standards

A.3.2.4 Oversight and Approval of Testers/Evaluators/Certifiers

For DT, the cognizant, developing organization (e.g., CPMO or JPMO in some cases) has oversight and approval. For OT, DOT&E has final oversight and approval on OSD oversight programs. For non-oversight programs, the services T&E Head Quarters (TEMA, AF/TE, OPNAV 091) have oversight and approval authority for their specific Service's OT&E. Depending on the certification, oversight and approval can range from the JPMO all the way up to the Joint Chiefs of Staff.

The NECC Joint Systems Team has the responsibility for designating the organizations / entities authorized to certify (i.e., validate) test results. It is expected that for each TEC criterion there will be one or more certification organizations / entities. For example, JITC would be the certifier of any interoperability test results as well as NR-KPP test results. (In the latter case, JITC would likely perform both tester and certifier roles, however that is the exception vice the rule.)

A.3.2.5 Tester/Evaluator/Certifier Business Processes When Interacting with the FDCE

The Business Process defined for FDCE participation by the TEC Community is developed by the T&E WIPT and JST. The below list provides examples of the types of processes the TEC Community will be called on to support via the FDCE. These functions are accessible from the FDCE Tester/Certifier page when an authorized user assigned the Tester/Certifier role logs into the FDCE:

1) Establishing CM certification criteria

2) Performing CM risk assessments

3) Managing CM certification processes

4) Reviewing and establishing technical and operational objectives

5) Reviewing events for T&E action and involvement

6) Reviewing CM pilot feedback from Warfighters

7) Managing user communities (e.g., who is authorized to "certify" specific TEC criteria)

8) Designating an OT lead for each CM Test Team (CMTT)

9) Assisting the JPMO in development of the TEMP, and TEMP annexes.

10) Providing input required to develop the TEMP Annex for each NECC CDP

11) Assisting the JST to execute the NECC Integrated T&E program by ensuring all Component-specific requirements are incorporated during each phase of testing

12) Evaluating operational effectiveness and suitability of the NECC CMs at the CDP and Increment levels

13) Exercising operational control and test management authority for Component-specific CMTTs IAW specific NECC or Component directives

14) Providing expertise to the JST on compliance matters affecting Operational Test and Evaluation (OT&E) policies

15) Reviewing DT plans, reports and relevant documentation for each CM

16) Monitoring CMs through the development and developmental piloting phases

17) Identifying how DT can be more operationally realistic so that DT result might be used to minimize redundancy and adequately scope the operational testing

18) Drafting, publishing, and coordinating operational test plans, reports, data management plans, etc IAW the JST-standardized format, as appropriate

19) Preparing independent operational evaluation reports IAW Component directives

20) Developing CDP-level Critical Operational Issues (COIs) for inclusion in the TEMP Annexes, in coordination with USJFCOM JCCD

21) Providing Component-unique resource requirements, test resource requirements, user requirements, test objectives, measures of effectiveness, performance and suitability (MOE/MOP/MOS) to the JST

22) Providing CM test plans and reports to support evaluation of COIs at CDP and Increment level

23) Applying the appropriate risk management methodology/tool at each CM or group of CMs to determine the required level of OT involvement, test to system, and Component-unique requirements

24) Assisting in the preparation and coordination of the deficiency reporting process

25) Conducting Component characterization and scoring for Reliability, Availability, and Maintainability (RAM) parameters during Component-specific testing, and provide results for the appropriate CM test report

26) Providing comments/recommendations in the development of the TEC criteria, as well as CPE events

27) Exercising operational control or test management authority over CM test teams IAW the JST charter.

28) Participating in the deficiency review process, if acting as CM OT Lead.

29) Consolidating test resource requirements by integrating test objectives and parameters for OT events

30) Conducting necessary Component-level operational tests.

31) Reviewing risk assessments for each CM, each CDP and each increment to determine level of OT involvement, and tests to system and Component-unique requirements

DRAFT

32) Coordinating with other OTAs to provide OT concept briefings and submit OT test plans to DOT&E

33) Coordinating JST efforts to ensure Verification, Validation and Accreditation (VV&A) requirements are addressed for all tools, models, simulations to be used for OT

34) Providing overall Integrated T&E expertise to NECC program management

35) Supporting JPMO Integrated T&E funding baseline efforts by providing timely OT funding requests and OT expenditure reports IAW Section 8.0 of this charter

36) Analyzing data to support NECC NR-KPP evaluations IAW DoD and Component regulations

37) Acting as Data and Test Documentation Manager for OT test plans and reports

38) Providing funding requirements to JPMO for NECC JST and OT events.

A.3.3 Warfighter

A.3.3.1 What Is a Warfighter?

The role of the Warfighter in the FDCE is defined in a number of ways with respect to the support that is offered up for the certification and assessment of CMs. The Warfighter role includes Warfighters from Combatant Commands, Joint Task Forces, Joint Force Components, Numbered Fleets, Numbered Air Forces, and Corps Service Combat Development and Battle Lab communities. Per the JCCD Warfighter Engagement Plan, the Warfighter is defined as follows:

1) Warfighter: Active Duty Military, Reserve or National Guard directly and/or recently engaged/involved in supporting Joint operations with pertinent functionalities. The Warfighter has current or recent experience as part of a Joint Force at the JTF HQ level plus or minus one (COCOM to JTF Component).

2) Warfighter Representative: Member of Title 10 and Joint organizations focused on C2 capabilities development, T&E and assessments, or monitoring of associated activities within boundaries of NECC.

3) Warfighter Surrogate: Individual with appropriate experience in COCOM, JTF, and/or Joint Functional Component C2 functions who could substitute for Warfighter in circumstances where actual Warfighter participation would be beneficial, but not required.

4) JFCOM Virtual Engagement Team (VET): A standing, virtual team of Warfighters, Warfighter Representatives, and Surrogates that provide the majority of Warfighting expertise needed for the NECC continuum of activities.

A.3.3.2 How Does One Become a Warfighter?

As the Warfighter Operational Sponsor for NECC, USJFCOM is the focal point for all new and emerging operational C2 needs, defining and articulating the detailed requirements needed to develop materiel solutions; and integrating and synchronizing DOTMLPF-P solutions with persistent cradle-to-grave engagement. The JCCD is currently developing a Warfighter Engagement Plan that formalizes the processes for Warfighter involvement in the NECC CM development cycle.

A.3.3.3 Warfighter Roles and Responsibilities

Warfighters supporting the NECC CM evaluation/testing may be resourced from various areas to include the JCCD for Joint Warfighters, and Service OTAs/CPMOs for Service Warfighters. The requirement for Warfighter support is established by the JST apportionment process of the tailored CM TECC. CM Test Teams (CMTTs) defines the scope of this support in the Detailed Test Plan (DTP) and a Requirements and Planning (R&P) matrix. The R&P matrix provides the details on Warfighter expertise, numbers of Warfighters, and dates of support. The JCCD and/or OTAs and CPMOs use these documents to activate their Warfighter engagement plan to acquire the Warfighters from various sources. Typical Warfighter responsibilities include the following:

1) Informally evaluating new capabilities as beta users
2) Participating in various piloting events to assess capabilities
3) Participating in the evaluation of available training modules/documentation
4) Identifying functional gaps between current capabilities and emerging CMs
5) Providing insight on how CMs are used to support TTP/Standard Operating Procedures (SOP)
6) Providing feedback on how current TTP/SOP may impact CMs
7) Managing NECC requirements (applies to the DOT_LPF-P role only)
8) Defining and refining policy, SOP, TTPs *(applies to the DOT_LPF-P role only)*
9) Providing subject matter expertise to the JST on matters concerning compliance with Joint operational requirements
10) Preparing joint Critical Operational Issues with OTAs and ensure COIs are documented in the TEMP Annex associated with each CDP
11) Providing input to selected JST reports to generate CDP summary test reports
12) Developing, coordinating, and providing JCD independent fielding recommendations for NECC CMs
13) Coordinating with Combatant Commanders, Services and Agencies to support JST validated requirements for Warfighter engagement throughout the CPAS process
14) Monitoring CMs through the Development, Developmental Piloting and Operational Piloting phases
15) Providing input to the TEMP, TEMP Annexes, and other Integrated T&E documentation.

A.3.3.4 Oversight and Approval of Warfighters

The JCCD-developed Warfighter Engagement Plan defines how Warfighters are solicited, selected, and approved for participation in NECC CM assessment activities. Key to this plan is the results of the TEC apportionment process which is conducted by the JST for each CM. Through apportionment, CPAS events are identified along with an initial estimate of required Warfighter participation for all testing activities. This estimate is updated in the follow-on TEMP annex and the CM test planning process. Specific Warfighter participation needs for formal OT events will be noted in the CM's detailed test plan.

DRAFT

A.3.3.5 Warfighter Business Processes when Interacting with the FDCE

The Business Process defined for FDCE participation by the Warfighter Community is developed by the JCCD. The below list shown in Figure 13 provides examples of the types of processes the Warfighter Community is called on to support via the FDCE. These functions are accessible from the FDCE Warfighter page when an authorized user assigned the Warfighter role logs into the FDCE:

1) Providing access to data on CMs (for example, a notice could be posted or announcement broadcast informing interested Warfighters that a new Weather CM will soon be available for their review)
2) Supporting pilots and tests of new CMs
3) Providing feedback on CMs
4) Establishing community Service Level Offerings (SLOs)
5) Managing Warfighter feedback on CMs
6) Accessing training; Warfighters can use the FDCE to access on-line or embedded training and to provide feedback on the usability and efficacy of that training
7) Coordinating and scheduling activities of interest to the Warfighter Community.

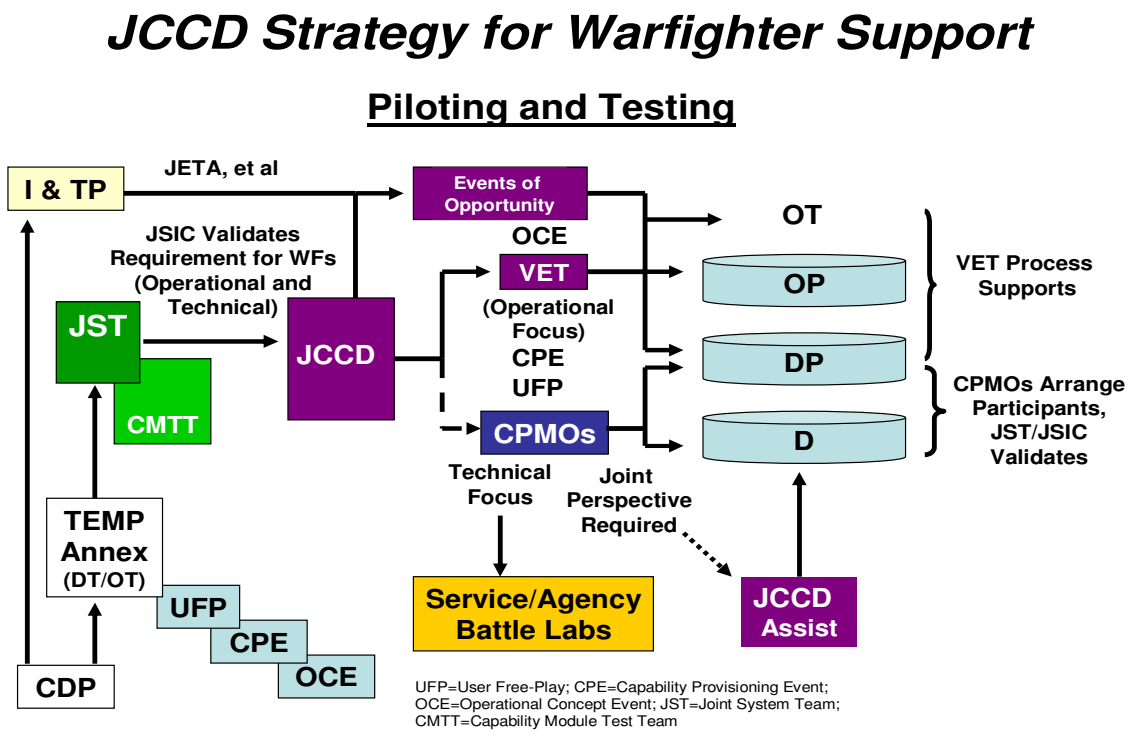

Figure 13: JFCOM Warfighter Engagement Strategy

APPENDIX B – USER ACCOUNT APPROVAL PROCESS

The process described below (User Account Approval Process) details the actions implemented by the JPMO and FDCE to manage users entering the FDCE. Validation checks are made to ensure proper user registration, and new users are directed to a registration page to apply for an account. The approval process ensures only valid accounts are then created.

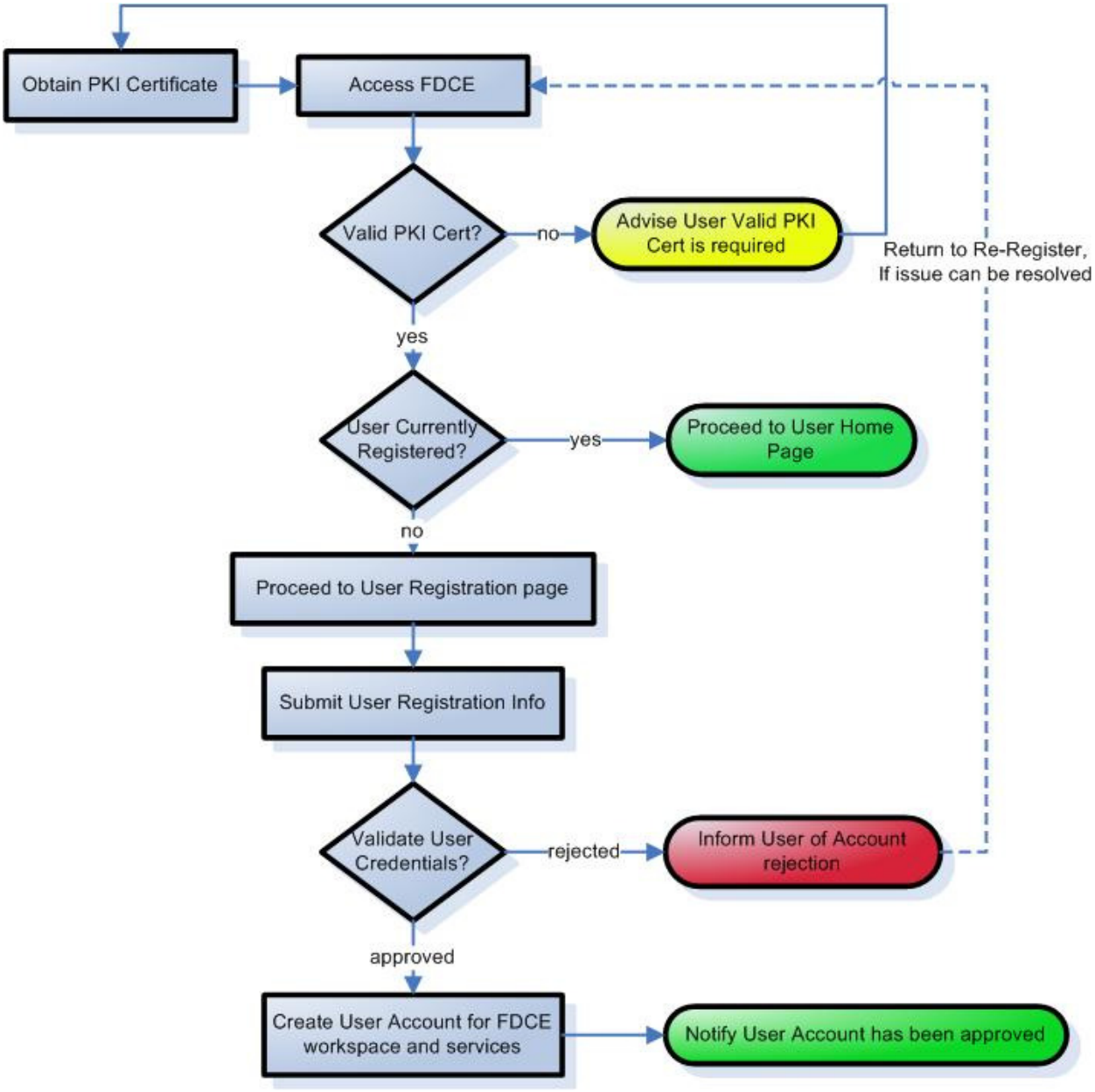

Figure B-1: User Account Approval Process Diagram

APPENDIX C – TOOLS ACQUISITION PROCESS

The flowchart below describes the process the JPMO has in place to support the tools acquisition process. This process enforces the necessary controls to ensure a consistent, repeatable set of actions are in place to provide the required oversight and review of nominated tools.

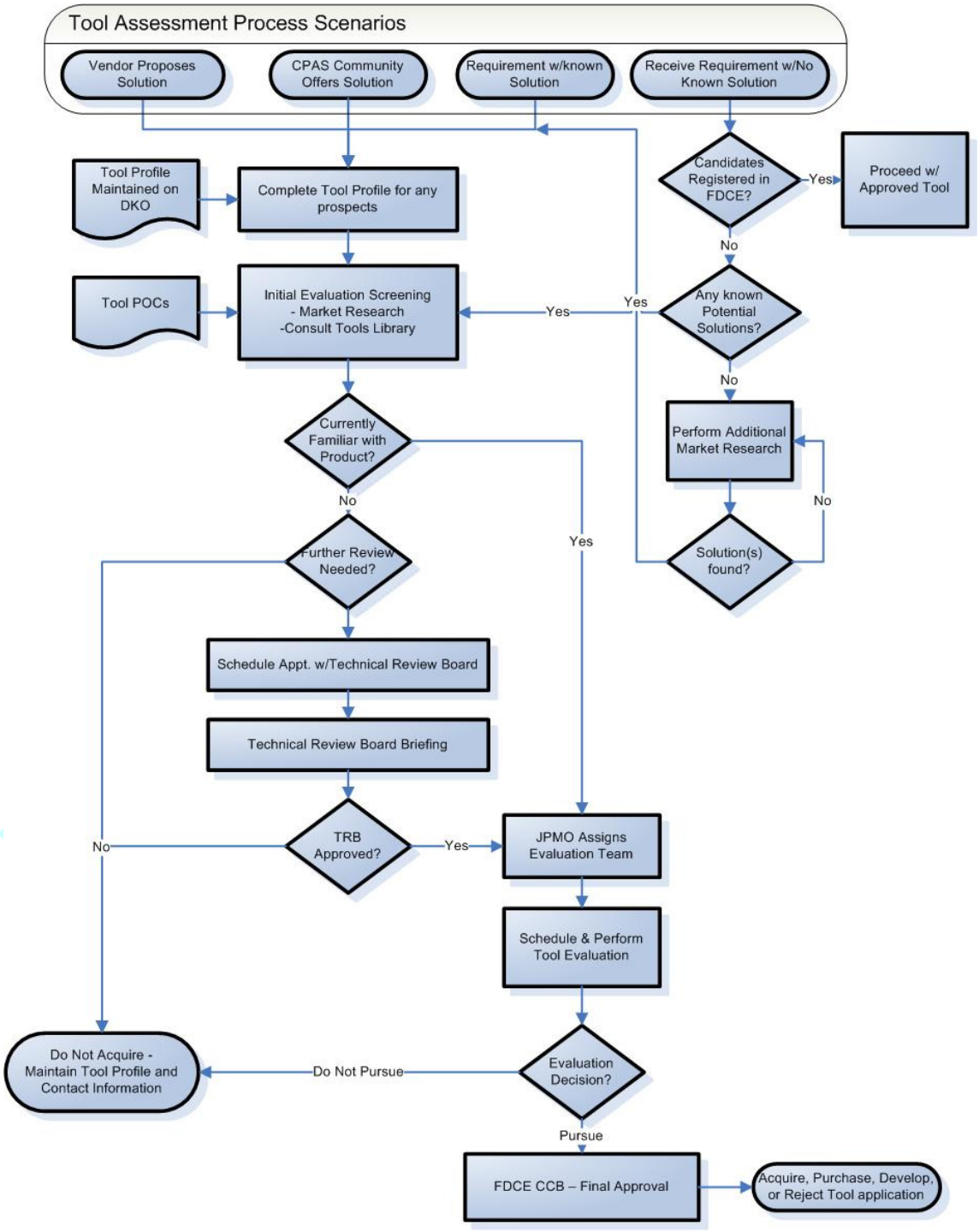

Figure C-1: Tool Assessment Process Scenarios Supporting Tool Acquisition Process

APPENDIX D – FDCE TOOLS APPLICATION

NECC FDCE Tools Profile

The tools profile helps us collect requirements for tools in a structured, repeatable manner. It also provides GOTS and COTS "vendors" with a formal mechanism for advertising their applicable product offerings.

Those who want to advertise a tool for use by the NECC Community need to fill out a "Tool Profile". This profile is an on-line form that asks for detailed information about the tool, such as:

1) Functional Category (IA, Testing, Configuration Mgmt, etc.)
2) COTS or GOTS
3) Accredited for NIPR? SIPR?
4) Validated by some authoritative entity?
5) In use by other DoD programs?
6) Training or specialized expertise required to effectively use the tool?
7) Web-accessible?
8) Special hardware or software requirements? (for example, only runs on Unix boxes, user agent required on local machine, etc.
9) Vendor Data
    a) Vendor Name
    b) Vendor SME POC Contact Info
    c) Tool Name
    d) Version Number
    e) Tool Description
    f) Basic Description of functionality
        i) Description of the product/service's benefit to the NECC program, a Service Oriented Architecture (SOA), and/or its customers
        ii) Why the product/service is unique or, if it is not, what makes it preferable to competitors' offerings
        iii) How long has the product/service been offered or in production (product maturity)
        iv) Who are the current customers (Very helpful to list any DoD Components/Commands). Product/service used in any DOD deployment/exercises/environments?
        v) What is the cost/pricing model, licensing structure for the product/service (e.g., fee for service, enterprise license exists, etc,)?
        vi) Note any government certifications for the product/service, e.g. NIAP, FIPS, etc.
    g) Maintenance Availability/Cost

DRAFT

h) Usage Rationale (i.e., what would NECC use this for?)

i) Vendor Website

j) Applicable Standards (perhaps a pull-down menu from out test, evaluation, and certification criteria list?) Also note additional standards and work with standards bodies.

NECC FDCE Tools Requirements Profile

A stakeholder who has a requirement for a tool must fill out a tools requirement profile which asks for the following details:

1) Functional Category (IA, Testing, Configuration Mgmt, etc.)
2) Usage Rationale (i.e., what do you need this tool to do?)
3) Must the tool be accredited for NIPR? SIPR?
4) Must the tool be validated by some authoritative entity?
5) Do you know of a tool currently in use by other DoD programs that fulfills your requirement? If so, please provide details.
6) Must the tool be web-accessible?
7) Must the tool run over the WAN?
8) Must the tool accommodate any special hardware or software requirements?
9) What standards must the tool comply with? (perhaps a pull-down menu from out test, evaluation, and certification criteria list?)
10) Does the tool need to interface with any existing systems/tools/processes? If so, what are they?
11) What is the required timeframe, i.e., when is this tool needed?
12) Which organizations will use the tool (e.g., Certifier, CPMO, etc.)
13) How many users/organizations do you estimate will use this tool?

DRAFT

APPENDIX E – FDCE LABORATORIES AND FACILITIES PROFILE

NECC FDCE Laboratories and Facilities Profile

This profile helps us to collect requirements for laboratories and facilities in a structured, repeatable manner. It also provides prospective NECC partners with a formal mechanism for advertising their applicable product offerings in the area of developmental laboratories and integration and test facilities.

Those who want to advertise a laboratory or facility for use by the NECC Community will need to fill out the following profile. This profile is an on-line form that asks for detailed information such as:

1) Functional Category (Developmental Testing, Integration, Operational Testing, etc.)
2) Government or Contractor
3) Accredited for NIPR? SIPR?
4) Validated by some authoritative entity?
5) In use by other DoD programs?
6) Training or specialized expertise required to use or to operate the laboratory or facility?
7) Web-accessible?
8) Special hardware or software requirements? (for example, only runs on Unix boxes, user agent required on local machine, etc.
9) Provider Data
    a) Name
    b) POC Contact Info
    c) Laboratory/Facility Name
    d) Description
    e) Basic Description of Services Provided:
        i) Description of the product/service's benefit to the NECC program, a Service Oriented Architecture (SOA), and/or its customers
        ii) Why the product/service is unique or, if it is not, what makes it preferable to competitors' offerings
        iii) How long has the product/service been offered or in production (product maturity)
        iv) Who are the current customers (Very helpful to list any DoD Components/Commands)?
        v) Service used in any DOD deployment/exercises/environments?
        vi) What is the cost/fee/pricing model?
        vii) Note any government certifications for the service, e.g. NIAP, FIPS, etc.
    f) Maintenance Availability/Cost

DRAFT

g) Usage Rationale (i.e., what would NECC use this for?)

h) Website

i) Hardware specifications, bandwidth, security requirements, ports and protocols (as applicable), physical and logical laydowns, etc.

j) Description of system administration/support/Help Desk capabilities

k) Hours of operation – specify constraints, if any

l) How many concurrent events can you support and of what scope/size?

m) Is there a published schedule or usage coordination support?

DRAFT

APPENDIX F – C2 CAPABILITY CATALOG METADATA

	Profile Area	Comments
I	**Functional**	
	Mission Areas	Choose From: Force Projection (Planning - JOPES; Deployment/Redeployment) Force Readiness (SORTS) Intelligence Situational Awareness Force Employment - Air/Space Operations, Land Operations, Maritime/Littoral Operations Force Protection Cross Functional/Infrastructure
	Component Name	The GCCS FoS is comprised of software modules packaged in accordance with COE guidance as COE segments. Segments are grouped into Components by one of two methods: 1. The segments provide a functional capability 2. The segments provide a set of services used by one or more other Components
	Component ACRONYM/Prefix (If Any)	
	Version Number	
	Planned Release(s)	Includes planned future capability enhancements and patch updates
	NECC Baseline Candidate	Does the GCCS FoS feel that segment/component should be a candidate for the NECC provisional baseline? Also include Submission/Approval status. Note: Trying to document existing FoS system. Even if component will not be considered for NECC, it needs to be known
	Description	A description of what the component does
	What NECC CDD requirements does it meet and how?	Refer to NECC CDD Appendix E, level 3 requirements
	What NECC Capability Module (CM) is this a possible candidate for?	Refer to the "Planned NECC Increment 1 CMs" slide V1.1 dated 5 Feb 07 (or later)
	What GCCS FoS (or C2) is it used in?	GCCS-J, M, A, AF?
	What existing FoS requirement does it fulfill?	Reference ORD or FoS CDD
	What DODAF views and/or information exist?	What DODAF views (OVs, SVs, TVs) and information and their location as
	Which NECC Key Performance Parameters are met?	The KPPs with numerical values have their threshold values shown in Table 6-2 NECC CDD dated 14 Feb 2007

DRAFT

	KPP# 1 Shared Situational Awareness	Compliance based on definition in Table 6-2 NECC CDD dated 14 Feb 2007. Tell if it complies and how it does so.
	KPP# 2 Planning	Compliance based on definition in Table 6-2 NECC CDD dated 14 Feb 2007. Tell if it complies and how it does so.
	KPP# 3 Training Support	Compliance based on definition in Table 6-2 NECC CDD dated 14 Feb 2007. Tell if it complies and how it does so.
	KPP# 4 Net Ready	Compliance based on definition in Table 6-2 NECC CDD dated 14 Feb 2007. Tell if it complies and how it does so.
II	**Technical**	
	Show software system block diagram for the component's relation in GCCS FoS	Use DODAF views if available and detailed enough. Otherwise provide whatever format is available.
	Show software system block diagram for the components internal operation	Use DODAF views if available and detailed enough. Otherwise provide whatever format is available.
	List Application(s) that is associated with/under this Component	Please use comma separated format of application prefixes
	Show what segments make up the component; title, description, version number	Please use comma separated format of segment prefixes for the segment lists below
	Segment name(s)	
	What are the component dependencies	What other component and or segments are required for successful operation. Typical SV-1 and SV-6 information
	Input Dependencies	The information inputs received by this component from other components
	Component Name	Component name inputs are received from
	Segment name	Segment name input received from
	Segment Version	
	Information received	Information exchanges
	Output Dependencies	What information this component sends to other components
	Component Name	Component name output sent to
	Segment name	Segment name output sent to

DRAFT

	Segment Version	Segment version output sent to
	Information sent	information exchanges
	What OS Platform(s) are used	What is the operating system that the segment operates on; SUN, Windows XP, Windows 2000, Unix, etc.
	Windows Client Version	
	Windows Client dependencies	Need know if there are any Windows specific dependencies (e.g., Win32 APIs, Windows DLLs, etc.)
	Windows Server Version	
	Windows Server dependencies	Need know if there are any Windows specific dependencies (e.g., Win32 APIs, Windows DLLs, AD, etc.)
	Solaris Client Version	
	Solaris Client dependencies	Need know if there are any Solaris specific dependencies (e.g., link libraries, security, etc)
	Solaris Server Version	
	Solaris Server dependencies	Need know if there are any Solaris specific dependencies (e.g., link libraries, security, etc)
	NECC IA Requirements Met	NECC IA Strategy (TBD) This will be expanded into additional IA requirements
	What are the communications infrastructure requirements?	Reflected in SV-2 type view. What communication systems are needed to have the component operate? If the component is hardwired to a communication system (such as a serial connection) that should be noted.
	What data sources does it use?	What database sources does it interface with; MIDB, Track DB, weather DB, etc.
	COTS Product needed for component to function	Commercial product(s) name, manufacturer, version number
	Security Classification	Commercial product(s) name, manufacturer, version number, license cost
	What SOA standards does it meet?	Use list from NECC TV-1. Provide FoS TV-1 if available, may also be done as a NESI technical compliance
III	**Programmatic**	
	FoS PMO POC	Who to contact on programmatic and business model information; name, address, phoned, email
	Funding Source(s) and appropriate PE/ project within the PE	Key item. (Sources other than PE58) Describe any other external funding sources or business model that supports this application.
	FYDP budget for: R&D and for O&M/ Sustainment	Budget: actual and projected, funding type. This information is not required for FoS members.

DRAFT

	Requirements Owner - Office Code, PH #, and current POC	Key item. Need to know for requirements transition
	Operational Sponsor - Office Code, PH #, and current POC	
	Source/Maintainer POR for Segment/Software: Contact Information	Some applications while used by one or more FoS Systems actually come from other programs - we need to know the source and who is maintaining them. Example METOC
	Developer Information	Provide summary of the actual contracted or tasked developer for the component and who they are under contract to.
	Technical SME POC	Who to contact for technical information about the component.
	Where fielded - (physical sites)	OV-5 is acceptable (or SV-1)
	Existing Data Rights	Government Purpose Rights, Unlimited Rights, or other. Who has the authority to distribute the component?
	Market Acceptance	How widely is the component used and accepted?
	Software Lifecycle (Maturity Phase)	Is the component in development phase, maintenance or end of life? If end of life is there a replacement identified?
	Location of technical baseline material and POC	The location of any technical material, POC and how to get access to it. SVD, SDD, ISP, SUM, SAG
	Available Training	Description of training available and by whom: embedded, on line, school house, OJT, POC
	Documentation	What documentation is available, and in what format (PDF, Word, HTML)? ▪ Users Manual ▪ Quick Reference Guide ▪ Software Administration Manual
	Help/Support	What support structure is available? ▪ Help Desk ▪ Feedback embedded links ▪ Email support
	CBT/Web-Based	Please describe the available training: ▪ Materials (PowerPoint, HTML) ▪ Delivery (CBT, WBT, Classroom) ▪ LMS capability ▪ SCORM/508 Compliant ▪ On-system or virtual training environment

DRAFT

	Schoolhouse	Please describe any existing training being taught and/or distributed in DoD Schoolhouses.
	Responsibility	Who is responsible for the development and delivery of the training content?
	Location	Where does the current training reside? Who has access to the training materials?
	Integrated Logistic Support (ILS) & Supportability	
	Location (hosting)	Where will this Capability Module be hosted? Choices are Enterprise Nodes or Local Nodes within the Service
	Location (support)	Where will the Help Desk support be located?
	Software (requirements impact)	What software applications will be required to be used?
	Software (data rights)	What data rights exist already and what additional data rights must be acquired and how often must software be updated?
	Hardware (updates and support)	How often must hardware be updated and how will existing hardware be supported?
	Operations	
	Help Desk Support	▪ Who to contact for assistance: name, phone number, email address, portal link
	Operation Center Support POC	▪ Who to contact regarding operations support: name, email address, phone ▪ Type of support available

DRAFT

APPENDIX G – ACRONYMS

Acronym	Description
ACTD	Advanced Concept Technology Demonstration
AFOTEC	Air Force Operational Test and Evaluation Center
ASD(NII)	Assistant Secretary of Defense for Networks, Information, and Infrastructure
ATEC	Army Test and Evaluation Command
ATO	Authority To Operate
C2	Command and Control
CA	Certification Authority
CAC	Combined Access Card
CARD	Cost Analysis Requirements Description
CCB	Configuration Control Board
CCD	Combat Capability Developer
CCDR	Combatant Commander
CDD	Capability Development Document
CDP	Capability Definition Package
CELCMC	Communications-Electronics Life Cycle Management Command
CM	Capability Module
CMTT	Capability Module Test Team
COCOM	Combatant Command
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
CONOPS	Concept of Operations
COTS	Commercial-off-the-Shelf
CPAS	Capability Provisioning Activities
CPE	Capability Provisioning Event
CPM	Capability Portfolio Manager
CPMO	Component Program Management Office
DAA	Designated Approval Authority
DDMS	DoD Discovery Metadata Standard
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry

DRAFT

Acronym	Description
DKO	Defense Knowledge On-Line Portal
DoD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
DOT_LPF-P	Doctrine, Operations, Training, Leadership, Personnel, Facilities and Policy
DOTMLPF-P	Doctrine, Operations, Training, Materiel, Leadership, Personnel, Facilities and Policy
DP	Developmental Piloting
DT	Developmental Testing
DTA	Development Test Agency
ESC	Electronic Systems Center
EMT	Engineered Mission Thread
ESM	Enterprise Service Management
FDCE	Federated Development and Certification Environment
FDCI	Federated Development and Certification Infrastructure
FDCP	Federated Development and Certification Process
FTP	Functionality Transition Plan
GCIC	Global Cyberspace Integration Center
GIG	Global Information Grid
IA	Information Assurance
IAWG	Information Assurance Working Group
I&TP	Integration and Technology Piloting
JCCD	Joint Combat Capability Developer
JCD	Joint Combat Developer
JCTD	Joint Concept Technology Demonstration
JDCAT	JSIC Data Collection & Analysis Tool
JITC	Joint Interoperability Test Command
JPM	Joint Program Manager
JPMO	Joint Program Management Office
JSIC	Joint Systems Integration Command
JST	Joint System Team
JTF-GNO	Joint Task Force-Global Network Operations
JWICS	Joint Worldwide Intelligence Communications System

DRAFT

Acronym	Description
LDAP	Lightweight Directory Access Protocol
MCCDC	Marine Corps Combat Development Command
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCSC	Marine Corps Systems Command
MDA	Milestone Decision Authority
MEF	Marine Expeditionary Force
MOA	Memorandum of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
MP	Materiel Provider
NCES	Net-Centric Enterprise Services
NECC	Net-Enabled Command Capability
NETOPS	Network Operations
NETWARCOM	Naval Network Warfare Command
NGA	National Geospatial-Intelligence Agency
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NR-KPP	Net Ready – Key Performance Parameter
NSA	National Security Agency
OCE	Operational Concept Event
OMT	Operational Mission Thread
OP	Operational Piloting
OT	Operational Test
OTRR	Operational Test Readiness Review
PEO	Program Executive Office
PKI	Public Key Infrastructure
PMO	Program Management Office
RAM	Reliability, Availability, and Maintainability
SSA	Shared Situational Awareness
SSC	SPAWAR Systems Center
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLO	Service Level Offering

DRAFT

Acronym	Description
SME	Subject Matter Experts
SOA	Service Oriented Architecture
SOP	Standard Operating Procedures
SPAWAR	Space and Naval Warfare Command
SPS	Service Specification(s)
T&E	Test and Evaluation
TBD	To Be Determined
TEC	Test, Evaluation, and Certification
TEMP	Test and Evaluation Master Plan
TRADOC	Training and Doctrine Command
TTP	Tactics, Techniques and Procedures
UDDI	Universal Description, Discovery, and Integration
UDOP	User-Defined Operational Picture
UFP	User Free Play
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
VET	Virtual Engagement Team
W3C	World-Wide Web Consortium
WIPT	Working Integrated Product Team
WS-I	Web Services Interoperability
XTT	Executing Test Team

DRAFT

APPENDIX H – REFERENCED DOCUMENTS

NECC DOCUMENT	DESCRIPTION	MILESTONE NEEDED	GOVERNMENT POC
Capabilities Development Document (CDD), 7 June 07	Documents NECC capabilities, requirements, and performance attributes as part of an evolutionary development strategy	MS B	USJFCOM
Configuration Management Plan (CMP), TBD	What is supposed to be produced, what is being produced, what has been produced, and what modifications have been made to what was produced.	MS B	NECC Operations & Integrated Logistics Support Branch
Cost Analysis Requirements Description (CARD), 20 Jun 2007	The CARD documents technical cost drivers to support economic analysis	MS B	NECC Program Control Branch
Developer Guidance Document, TBD		MS B	NECC System Engineering Branch
GCCS Family of Systems (FoS) to NECC Functionality and Transition Plan	Identify the process, criteria, and schedule for the migration of existing GCCS FoS functionality	MS B	NECC System Engineering Branch
Information Assurance Strategy (IAS), Version 1.0, 12 Dec 2005	Strategy for implementing IA requirements and processes into NECC.	MS A	NECC System Engineering Branch
Information Support Plan (ISP), TBD	Information-related needs in support of the operational and functional capabilities	MS B and C	NECC Operations and Integrated Logistics Support Branch
Integrated Baseline Review (IBR), April 2006	Provides overview of plan for the TD Phase, Baseline Work Packages, Integrated Master Schedule (IMS) and Budget. The IBR includes performance management and performance metrics	Each Major Milestone and as required by the PM	NECC Program Control Branch
Integrated Master Schedule (IMS), Updated on a monthly basis	Networked multi-layered schedule that includes all IMP events, accomplishments, and criteria, in accordance with the program WBS.	Each Major Milestone and as required by the PM	NECC Program Control Branch
NECC C2 Cross-COI Data Strategy, TBD	Developed in accordance with DoD Net-Centric Data Strategy.	MS B	NECC System Engineering Branch
Net-Enabled Command Capability Systems Engineering Plan (SEP), Increment 1 Milestone B, Version 1.0 dated 9 August 2007	Systems engineering processes and the integration of the process with the management, support, and acquisition processes	MS B	NECC
Program Protection Plan (PPP), TBD	Protection efforts for denying unauthorized access to and for preventing inadvertent disclosure of NECC program information.	MS B and C	NECC Program Control Branch

DRAFT

NECC DOCUMENT	DESCRIPTION	MILESTONE NEEDED	GOVERNMENT POC
Risk Management Strategy and Plan, 28 March 2007	Life cycle risks and presents an approach for risk mitigation	MS B	NECC Program Control Branch
Technical Transition Architecture, Version 0.71, 20 Dec 2005	Approach for achieving the NECC Technical Transition Architecture	MS B	NECC Chief Engineer
Technology Development Strategy (TDS), Version 1.0, dated 16 December 2005	The TDS reduces technology risk and documents the appropriate set of technologies to be integrated into a full system	MS A, B and C	NECC System Engineering Branch
Test and Evaluation Master Plan (TEMP)	Details of the approach, functions, roles, and responsibilities for testing NECC capabilities	MS B and C	NECC Test & Evaluation Branch
Test and Evaluation Strategy (T&ES), Version 1.0, 16 Dec 2005	The NECC Test and Evaluation (T&E) strategy is consistent with the incremental development approach, as specified in the CDD. The strategy includes Test and Evaluation stages associated with NECC ECM Development Phases.	MS A	NECC Test & Evaluation Branch
The NECC Concept for Rapid Provisioning of C2 Capabilities onto the GIG, April 2006	The development and delivery of C2 capabilities onto the Global Information Grid (GIG) must be conducted as an integral part of overall GIG operations. Currently there is a developing notion of operating capabilities on the GIG called Network Operations (NETOPS). The NECC program is proposing to extend the concept of GIG operations to include Capability Provisioning Activities (or CPAS)		NECC Chief Engineer

DRAFT

APPENDIX I – FDCE 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.***CI***		
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 FDCE requirements including whether this is in/out of the scope of the FDCE 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		

DRAFT

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***

DRAFT

APPENDIX J – FDCE HARDWARE CONFIGURATION

The suite of equipment is the same for each of the networks (Internet, NIPRNet, & SIPRNet) and consists of multiple servers to run the portal and database software. The infrastructure that supports the FDCE Information Portal requires minimal physical hardware and is scalable in a linear fashion. Additional infrastructure is required for NECC-provisioned tools, such as SOA test tools made available to developers and testers post-Milestone B.

The hardware configuration to support the FDCE Process consists of SUN X22OO Blade systems which run the following servers:

1) Web Server
2) MySQL Database
3) Lightweight Directory Access Protocol (LDAP) Server

The Web Server is running Apache 2.2.x with a Mongrel Web Server to which the FDCE Rails application is deployed. This Web Application is accessed via 2-Way SSL over port 443 by an approved user base. The FDCE application is deployed to this Web Server. All persistent information used by the FDCE Navigator is stored in the MySql database. This includes data for capabilities, events, requirements, profiles, proposals, responses, users, groups, roles, tools, comments, and registration requests and associations between these entities. User information does not include any password information but does contain the DN (Distinguished Name) of the PKI certificate with which the user registered.

DRAFT

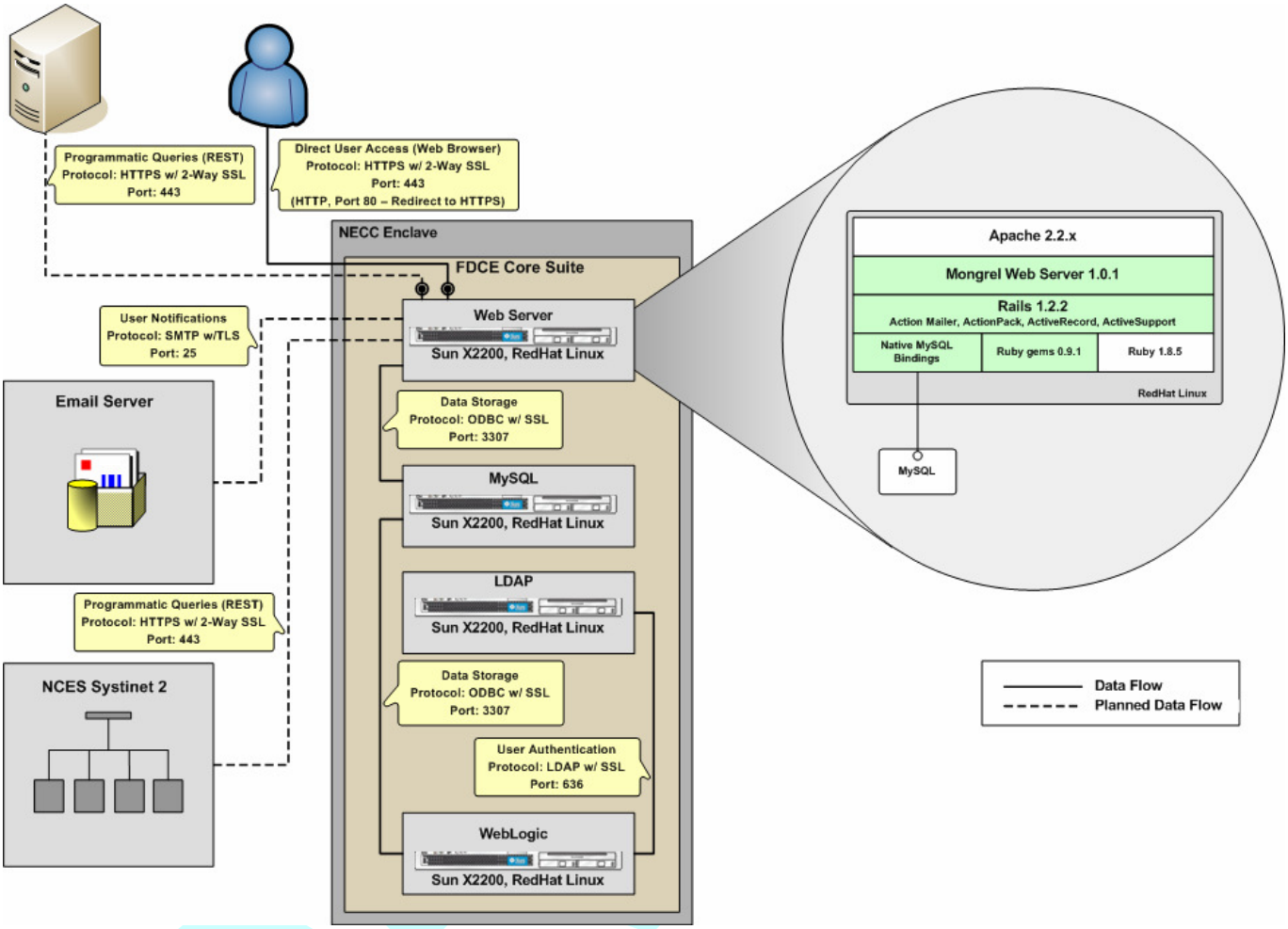

Figure 14: FDCE Deployment Hardware

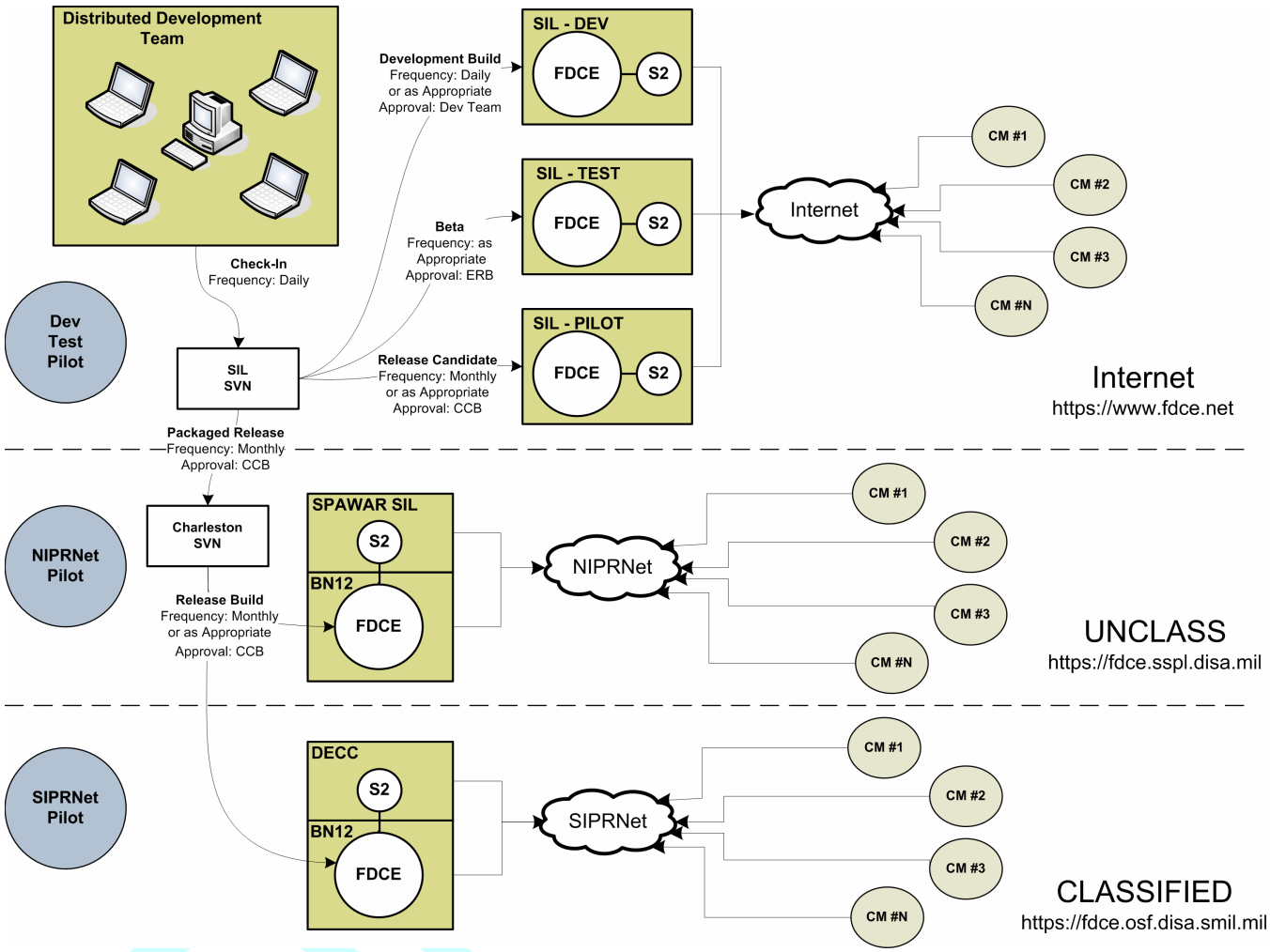

Figure 15: FDCE Deployment by Enclave