

UNCLASSIFIED



**Net-Enabled Command Capability
INCREMENT 1 CAPSTONE
TEST AND EVALUATION MASTER PLAN
(TEMP)
Version 1.0
6 August 2007**

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 Managers for Navy, Air Force, Army,
Marine Corps, JFCOM, and DISA

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

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

UNCLASSIFIED

UNCLASSIFIED

APPROVAL PAGE

Submitted by:

Laura D. Knight

Date: 06 Aug 07

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

Concurred by:

Michael Spencer by direction

Date: 16 Aug 2007

MICHAEL SPENCER
Program Manager,
Navy Component Program Management Office (CPMO)
Net-Enabled Command Capability (NECC)

Concurred by:

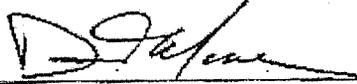
Linda W. Harris, DCPM

Date: 16 Aug 07

for STEVE WEBB
Colonel, USAF
Program Manager,
AF Component Program Management Office (CPMO)
Net-Enabled Command Capability (NECC)

UNCLASSIFIED

Concurred by:



Date: 16 Aug 07

DAVID M. MOORE
Colonel, USA
Program Manager,
Army Component Program Management Office (CPMO)
Net-Enabled Command Capability (NECC)

Concurred by:



Date: 15 Aug 07

JOSEPH D. BROWN
Colonel, USA
Program Manager,
DISA Component Program Management Office (CPMO)
Net-Enabled Command Capability (NECC)

Concurred by:



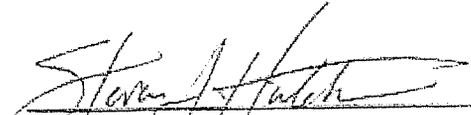
Date: 280819

BRIAN P. ELSTAD
Lieutenant Colonel, USMC
Program Manager,
USMC Component Program Management Office (CPMO)
Net-Enabled Command Capability (NECC)

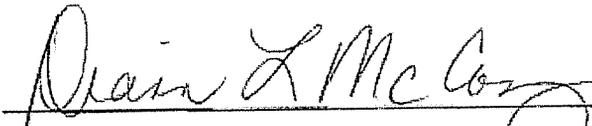
UNCLASSIFIED

Concurred by:  Date: 7 Aug 07

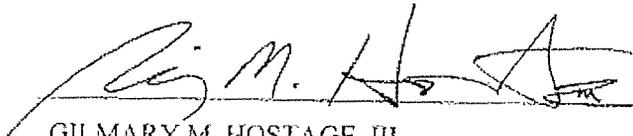
DAVID B. BENNETT
Deputy, Program Executive Office,
Command and Control Capabilities (PEO, C2C),
Defense Information Systems Agency (DISA)

Concurred by:  Date: 8 Aug 07

STEVEN J. HUTCHISON
Test and Evaluation Executive,
Defense Information Systems Agency (DISA)

Concurred by:  Date: 9 Aug 07

DIANN L. McCOY
Component Acquisition Executive (CAE)
Defense Information Systems Agency (DISA)

Concurred by:  Date: 13 Aug 07

GILMARY M. HOSTAGE, III
Major General, USAF,
Director, Joint Capabilities Development/J8
U.S. Joint Forces Command (JFCOM)

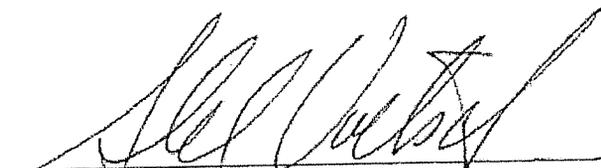
UNCLASSIFIED

Concurred by:  SES Date: 24 Aug 07

ROGER A. NADEAU
Major General, USA
Commanding General, Army Test and Evaluation Command
(ATEC)

Concurred by:  Date: 30 Aug 07

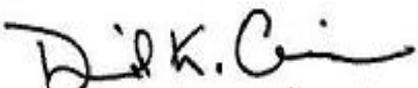
STEPHEN T. SARGEANT
Major General, USAF,
Commander, Air Force Operational Test and Evaluation Center
(AFOTEC)

Concurred by:  Date: 22 August 2007

STEPHEN S. VOETSCH
Rear Admiral, USN,
Commander Operational Test and Evaluation Force
(COMOPTEVFOR)

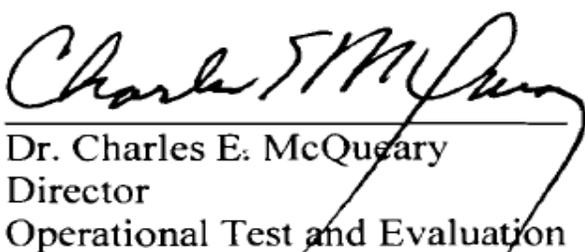
Concurred by:  Col USMC Date: 15/8/07

MICHAEL S. BOHN
Colonel, USMC,
Director, Marine Corps Operational Test and Evaluation
Activity (MCOTEA)

Concurred by:  Date: 27 AUG '07
FOR Deputy, Army T/E Executive
DR. HENRY C. DUBIN
Army Test and Evaluation Executive

Concurred by:  Date: 14 AUG 07
RONALD C. STEPHENS
Colonel, USA,
Commander,
Joint Interoperability Test Command (JITC)

Approved by:  06 Dec 07
Timothy J. Harp Date
DASD(C3ISR & IT Acquisition)
Acting

Approved by  18 DEC 2007
Dr. Charles E. McQuary Date
Director
Operational Test and Evaluation

EXECUTIVE SUMMARY

Net-Enabled Command Capability (NECC), originally named Joint Command and Control (JC2) Capability, is a Joint program led by Defense Information Systems Agency (DISA). NECC falls under the Office of the Secretary of Defense (OSD) oversight with the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense (DoD) Chief Information Officer (CIO) (ASD(NII)/DoD CIO) as the Milestone Decision Authority (MDA), as delegated by the Defense Acquisition Executive, and with other OSD offices, the Joint Staff, US Joint Forces Command (USJFCOM), other government agencies, and with the Army, Navy, Air Force, and Marine Corps.

The NECC program uses a two-tiered integrated test hierarchal approach organized by the lead Operational Test Agency (OTA), Army Test and Evaluation Command (ATEC). The Joint System Team (JST) is at the top of this tier. The JST is an O-5/O-6 working level organization with representation from all test and certification stakeholders whose roles and responsibilities are outlined in the JST Charter and are identified later in this Capstone Test and Evaluation Master Plan (TEMP). The second level of test hierarchy is the Capability Module Test Team (CM TT). The CM TT is composed of an OTA Lead and a Developmental Test (DT) Lead. The NECC Joint Program Management Officer (JPMO) has the primary responsibility for Developmental Test and Evaluation (DT&E) for this program. Each service Component Program Management Office (CPMO) will have specific responsibility for DT&E in their respective Service/Component/Agency. ATEC will coordinate test support and reporting requirements from the other operational test agencies. USJFCOM is the Joint requirements and operational sponsor representing the Warfighter for this program. To help mitigate program risk, maximize available resources, and support the agile fielding of incremental Command and Control (C2) capabilities, the JST will lead developmental and operational relevant test activities through a combined Developmental Test/Operational Test (DT/OT) approach. This combined test approach uses a virtual environment through the Federated Development and Certification Environment (FDCE) and Capability Provisioning Activities (CPAS) net-centric processes.

NECC is an Evolutionary Acquisition Program using an incremental development approach to develop capabilities over several increments. This increment level, Milestone B Capstone TEMP outlines the overall Test and Evaluation (T&E) program strategy that will guide the developmental and operational test efforts supporting this program and does not contain the level of detail that is ordinarily captured at system level TEMPs or Detailed Test Plans (DTP). This level of detail will be captured in subsequent TEMP annexes and will provide further detail in the following areas as they become available:

- Development and testing of Measures of Effectiveness and Suitability (MOE/MOS)
- Mapping of Key Performance Parameters (KPPs) to Critical Operational Issues (COIs)
- Detailed DT/OT Testing events to include matrices of CMs that will be tested
- Detailed DT/OT testing environments and scope

UNCLASSIFIED

- Identification of prototype, engineering development, pre-production, and production models to be tested
- Derived Information Support Plan (ISP) requirements used to support interoperability testing
- Modeling and Simulation (M&S) approaches to include threat simulators/simulations
- Development and testing of Critical Technical Parameters (CTP)
- Detailed T&E funding information for each phase of test
- Identification and roles and responsibilities of Integrated Product Teams (IPTs)
- Development and mapping of Interoperability Support Plans (ISP) at the Capability Definition Package (CDP) level
- Specific CM data collection and analysis processes
- Inclusion of Technical Readiness Reviews (TRR) major event and technical review dates
- Identification of configuration control and test data review boards and members
- Descriptions of specific testing environments and test facilities
- Testing Logistical support and Support Equipment requirements
- Operational and Maintenance documentation
- Joint and Allied Forces testing events and requirements
- Information Assurance and Anti-tamper testing requirements and approaches
- Detailed plans to evaluate environmental conditions not previously tested

This Increment 1 Capstone TEMP for the NECC program is submitted in accordance with the DoD Directive (DoDD) 5000.1, *The Defense Acquisition System*, the DoD Instruction (DoDI) 5000.2, *Operation of the Defense Acquisition System*, and specific direction contained in the NECC ADM dated 07 March 2006.

UNCLASSIFIED

REVISION HISTORY

VERSION NUMBER	REVIEWER / ORG	CHANGES	VERSION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGES
0.0.5.3	DLB/SPEC	Performed an initial edit of the entire document including acronyms Sent it back to author for review	22 May 2007	22 May 07	Dustan Brown
0.0.5.3	TJQ/T&E	Reviewed document edit, updates section 1, 2, and 3 content, added references, added hyperlinks, defined acronyms	24 May 2007	24 May 07	Tom Quinn Paul Pompier Robert Beaton
0.5.4	DLB/SPEC	Performed final edit and reformatted document to meet NECC template guidelines, added full acronym list, replace necessary graphics, added Approval page for signatures, inserted new AS text in section 2, inserted hyperlinks, and inserted headers/footers.	25 May 2007	25 May 07	Dustan Brown
0.5.5	RBG/BIT	Edit on acronyms, grammar, and consistency	22 June 2007	22 June 07	Becky Gardner
0.5.6	RBG/BIT	Final edit on acronyms, grammar, consistency, and formatting	24 June 2007	24 June 07	Becky Gardner
0.5.6	DLB/SPEC	Final edit check	24 June 2007	24 June 07	Dustan Brown
0.6.2	DLB/SPEC	Final edit for Senior Review. Formatted signature page.	16 July 2007	16 July 07	Dustan Brown
1.0	IGJ/BIT (NECC Documentation Support)	Reformatting and grammar edits. New figure (schedule) inserted and defined; figures and tables redefined so they present better; highlighted text that need correction/addition; headers and footers redefined; ensured the document format conforms to the approved template; new TOC generated.	3 Aug 2007	3 Aug 07	Issa Jones

TABLE OF CONTENTS

APPROVAL PAGEII

EXECUTIVE SUMMARY VII

REVISION HISTORY IX

1 SYSTEM INTRODUCTION 1

1.1 MISSION DESCRIPTION 1

1.2 SYSTEM DESCRIPTION 2

 1.2.1 Architecture Framework..... 2

 1.2.2 NECC Physical Overview 3

1.3 NECC SYSTEM BOUNDARY DESCRIPTION 4

1.4 INCREMENT 1 CM PROPOSED SCOPE OF EFFORT 5

1.5 PILOTING AND FEDERATED DEVELOPMENT AND CERTIFICATION ENVIRONMENT (FDCE) PROCESS OVERVIEW 6

 1.5.1 Capability Provisioning Activities 6

 1.5.2 Overview of the FDCE Environment 7

 1.5.3 Piloting Activities as Test Events 11

1.6 SYSTEM THREAT ASSESSMENT 12

1.7 KEY PERFORMANCE PARAMETERS 12

1.8 SYSTEM KPPs AS DETAILED IN THE CDD ARE SUMMARIZED IN TABLE 2 12

1.9 KSAS FOR INCREMENT 1 15

1.10 TEST, EVALUATION, AND CERTIFICATION CRITERIA 19

1.11 MEASURES OF EFFECTIVENESS AND SUITABILITY 20

1.12 CRITICAL TECHNICAL PARAMETERS/SERVICE PERFORMANCE SPECIFICATIONS 20

1.13 RISK AREAS AND RISK MITIGATION 20

2 INTEGRATED TEST PROGRAM SUMMARY 21

2.1 SCHEDULING 21

2.2 MANAGEMENT 22

 2.2.1 NECC Test Teams 22

 2.2.2 Assistant Secretary of Defense for Networks and Information Integration 25

 2.2.3 Designated Approval Authority for Information Assurance, USSTRATCOM 25

 2.2.4 Lead Component for the Net-Enabled Command Capability, DISA 25

 2.2.5 Joint Program Executive Office for the Net-Enabled Command Capability 25

 2.2.6 Joint Program Management Office (JPMO) for NECC 27

 2.2.7 Component Program Management Office 27

 2.2.8 U.S. Joint Forces Command 28

 2.2.9 Director, Joint Staff 30

 2.2.10 Director of Operational Test & Evaluation 30

 2.2.11 OUSD(AT&L) System Engineering/Assessment and Support DT&E 30

 2.2.12 Operational Test Agencies 30

 2.2.13 Developmental Test Agencies 34

 2.2.14 Information System Security Engineer 34

3 INTEGRATED TEST AND EVALUATION 35

3.1 NECC TEST HIERARCHY APPROACH 35

3.2 TESTING GOVERNANCE 35

3.3 INTEGRATED TEST AND EVALUATION CONCEPTS 36

 3.3.1 Requirements Phase 37

 3.3.2 Planning Phase 38

 3.3.3 Test Plan Development 39

UNCLASSIFIED

3.3.4 *Testing Phase*.....41

3.4 TEST RELATED DOCUMENTATION APPROVAL CHAIN CONSIDERATIONS46

3.5 FIELDING PHASE.....46

3.6 CRITICAL OPERATIONAL ISSUES.....48

3.7 T&E EVENTS/SCOPE OF TESTING/SCENARIOS.....48

3.8 MODELING AND SIMULATION.....49

4 TEST AND EVALUATION RESOURCES SUMMARY50

4.1 T&E FUNDING50

4.2 TESTING RESOURCES.....51

4.3 TEST ARTICLES51

4.4 TEST SITES AND INSTRUMENTATION51

4.4.1 *Test Sites*.....51

4.4.2 *FDCE Lab Facility and JPMO Developmental Hosting Facility*.....51

4.4.3 *Test and Production Facilities*.....52

4.5 FUNDING RESOURCES.....54

APPENDIX A – ACRONYMS57

APPENDIX B: GLOSSARY OF TERMS.....65

APPENDIX C: REFERENCED DOCUMENTS71

APPENDIX D: TEST, EVALUATION, AND CERTIFICATION CRITERIA76

APPENDIX E: REFERENCES.....77

APPENDIX F: POINTS OF CONTACT.....79

LIST OF FIGURES

Figure 1: NECC Architecture Framework 2

Figure 2: NECC Systems Communications Description 3

Figure 3: NECC Systems Interface Description (SV-1) 4

Figure 4: Certification Entrance Criteria for a CM and the Decision Makers 8

Figure 5: FDCE Stages 9

Figure 6: NECC Integrated Test Program Schedule 22

Figure 7: JPEO Organization 26

Figure 8: NECC T&E Strategy 37

Figure 9: CM/Increment 1 Fielding Process 47

LIST OF TABLES

Table 1: Increment 1 Logical List of CMs..... 5

Table 2: Key Performance Parameters..... 13

Table 3: Key System Attributes 15

NECC Increment 1 Capstone TEMP v1.0 2

UNCLASSIFIED

Table 4: NECC Program Report Summary..... 45
Table 5: JST Manpower/Funding Estimate 54
Table 6: Total NECC OTA Funding Estimates/FY 56
Table 7: CM TT Manpower Estimate..... 56

1 SYSTEM INTRODUCTION

1.1 Mission Description¹

The Net-Enabled Command Capability (NECC), as envisioned in Joint Vision 2020, will become the Department of Defense's (DoD) principal Command and Control (C2) information capability. The objective "mission space" for NECC is defined as the area supporting command capability and C2 activities from the National Military Command System (NMCS) through the Joint Task Force (JTF) and Service/Functional components to unit level commanders. NECC enables horizontal and vertical information flow and collaboration across this command spectrum. In addition, NECC exploits data from global expertise and information centers of excellence through reach-back functionality, based on net-centric services. NECC Increment 1 mission space extends from NMCS through Service/Functional Components with the focus on the Joint Force Commander (JFC) Situational Awareness (SA) and Joint operations planning.

NECC complements the integrated Joint warfighting force by empowering the C2 community and Joint Planning and Execution Community (JPEC) with the data and information needed to make timely and informed decisions. NECC decision superiority is enhanced by information and command support capabilities that provide the Warfighter with heightened situational awareness and the agility to plan, execute, monitor, and assess Joint and multinational operations throughout all levels of conflict.

NECC is an evolutionary family of services that merges current and new Warfighter C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. An integral part of this strategy is the transition of the Global Command and Control System (GCCS) Family of Systems (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 will integrate capabilities into a Service-Oriented Architecture (SOA) that includes applications and databases in accordance with [DoD Net-Centric Data Strategy](#).² Global Information Grid (GIG) Enterprise Services (GES) and Net-Centric Enterprise Services (NCES) will support NECC by enabling shared access to Service/Agency/Joint-provided services (data sources and applications).

NECC will provide enhanced access to shared data sources; thereby, enabling users to rapidly adapt to changing mission needs by defining and tailoring their information environment and using common sets of Joint capabilities resulting in efficient, timely, and effective command of forces and control of engagements.

The NECC Capability Development Document (CDD) provides the overall mission requirements for this Capstone Test and Evaluation Master Plan (TEMP). Subsequent Capability Definition Packages (CDPs) will be used to detail further derived mission requirements from the CDD and will be captured in TEMP Annexes to support development of future Critical Operational Issues (COIs) at the CDP level.

¹ Mission Description provided by USJFCOM JCCD.

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

1.2 System Description

1.2.1 Architecture Framework

Two levels of architectural guidance define NECC terminology per Figure 1 and provide broad direction on how NECC components should be designed and interact. NECC's overarching technical guidance is the Architecture Framework. The NECC Architecture Framework is intended to accomplish the following:

- Standardize NECC architecture terminology.
- Establish long-term NECC architecture objectives.
- Provide a long-term architectural road map to ensure near-term architectural and Systems Engineering (SE) decisions align with long-term NECC architecture objectives.
- Guide development of NECC increment-specific architectures and designs.

The five views of the NECC Architecture Framework are depicted below in Figure 1. Refer to [NECC Architecture Framework](#)³ for more information.

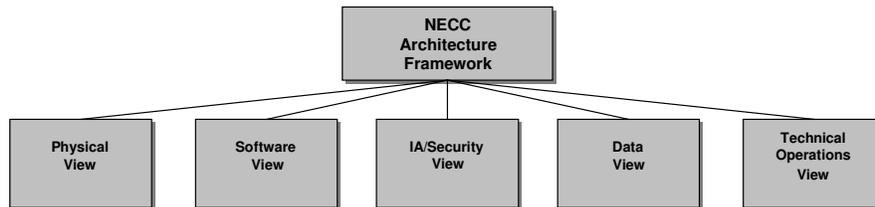


Figure 1: NECC Architecture Framework

NECC increment-specific architecture(s) provides the next level of increased detail beyond the Architecture Framework. In addition to the same views discussed in the Architecture Framework, an increment-specific architecture will include a context diagram and a technical standards view. The context diagram will depict the NECC increment system boundary with particular attention to external system and service interfaces and the dynamic relationships between NECC and the GCCS FoS. The technical standards view will include a list of technical standards applicable to each increment's design and will be organized along the five Architecture Framework views. The increment-specific Physical View will provide the physical layout of NECC components including enterprise nodes, local nodes, and appliances. The Physical View will also define the target hardware environment and specify how NECC software components will be hosted. The increment-specific Software View will define the standards for service interface specification and specify common infrastructure services such as redirection and orchestration. The Software View will also address considerations unique to NECC clients. The increment-specific Information Assurance (IA)/Security View will provide details on information assurance implementation, which includes authentication, authorization, and cross-domain solutions. The increment-specific Data View will provide additional detail on what data should be exposed, data standards and eXtensible Markup Language (XML) schemas, how to tag data, and the physical location of data assets. The increment-specific Technical Operations View

³ Architecture Working Group, Architecture Framework, 31, January 2007, Version 1.0, URL: https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

will provide additional detail on tracking service-level agreements, interface management, enterprise node and appliance management, and NECC Control Center requirements.

Within its architecture, the NECC concept of a local node explicitly accounts for NECC users with Disconnected/Intermittent/Limited-bandwidth (DIL) connectivity to the GIG. The NECC implementation will provide DIL users with local computing resources (processors, business logic, and cached data) necessary to meet immediate high-priority needs. DIL requirements will be explicitly considered during the development of each Capability Module's (CM's) Requirement Baseline. As a result, DIL impacts both NECC system design and component deployment locations.

1.2.2 NECC Physical Overview⁴

The NECC architecture reflects a set of distributed software components that are designed to operate in concert across the GIG (see Figure 2). NECC software components are designed to operate on a standard GIG Computing Node (GCN) as defined in the NECC Increment 1 Architecture specification.

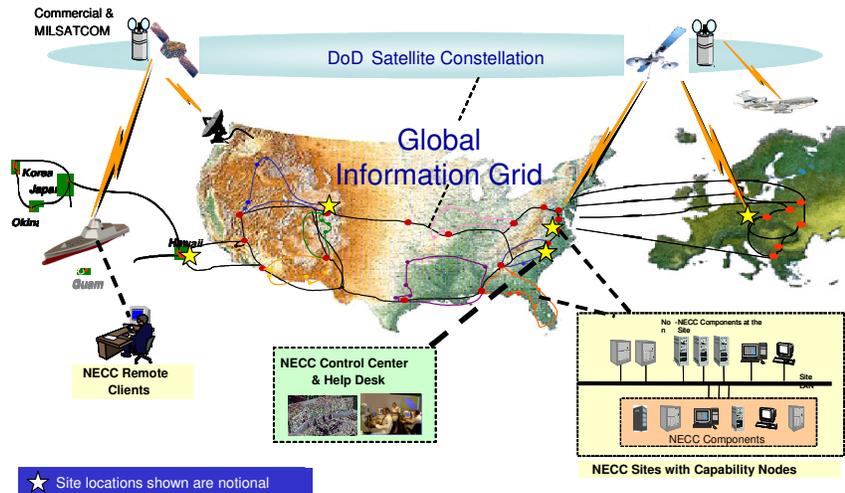


Figure 2: NECC Systems Communications Description

Physically, NECC consists of four types of entities/components:

- **NECC Capability Modules** – a NECC CM is the primary test article of the NECC program. It is a collection of one or more services that provide an operationally useful capability. From a consumer's point of view, CMs may be perceived as “black boxes” on the network in that their internal implementation is hidden from the consumer. A CM can be a standalone capability, or it can contribute to the execution of a mission thread interacting with other CMs.
- **NECC Clients** - they include NECC developed clients (software provided by NECC, and in some cases hardware), clients transitioned from GCCS FoS, and third-party clients such as browsers and other commercial client software.

⁴ Reference USJFCOM Capability Development Document, 07 June 2007, v1.0

- **NECC Sites** – an NECC Site is a physical place (connected to other sites via the GIG) where one or more NECC components are hosted. These components are the computing platforms that support the Capability Nodes.
- **NECC Capability Nodes** - Capability Nodes can be implemented on different types of platforms, such as a single server, grid computing hardware, clustered servers, or even a client workstation.

1.3 NECC System Boundary Description⁵

Figure 3 shows the NECC Systems Interface Description (SV-1). It depicts the boundary between NECC software components and the hardware that NECC software components run upon, and NECC software components and other software systems with which NECC must interact.

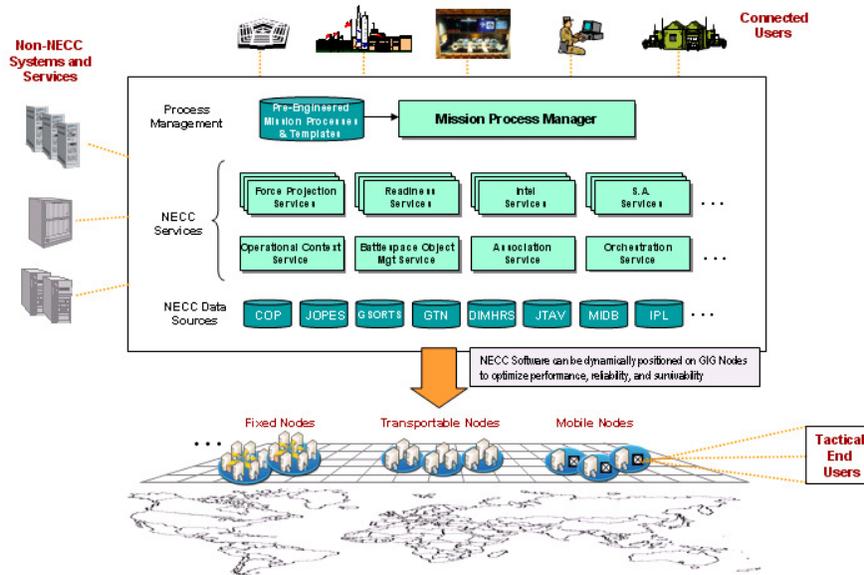


Figure 3: NECC Systems Interface Description (SV-1)

With respect to hardware, NECC software is being designed to run in a variety of operational environments including fixed sites, transportable sites, and mobile sites. The current concept is to align with a standard GCN architecture that is implemented in all three environments. A key part of the GCN architecture is the use of virtual machine environments to allow NECC software components to run safely across all types of environments.

With respect to other software systems, NECC software will interact with a variety of information systems including (but not limited to) the intelligence, logistics, transportation, medical, and geospatial communities. Included in the category is the use of Core Enterprise Services (CES) provided by NCES. NECC software will interact with other services in one of two ways. The primary interface mechanism will be to do service-to-service interactions in accordance with the DoD Net-centric Data Strategy. Where this is not achievable in the short

⁵ Reference USJFCOM Capabilities Development Document, 07 June 2007, v1.0

run (due to program schedules), NECC in some instances will implement temporary point-to-point interfaces until service-to-service interfaces become available.

1.4 Increment 1 CM Proposed Scope of Effort⁶

Table 1 provides a crosswalk of Increment 1 CMs to CDPs. As CMs are selected for development, additional information will be provided in their respective CDP TEMP Annexes.

Table 1: Increment 1 Logical List of CMs

Capability Module	Mission Area from CDD	CDP Reference
Deployment Plan Management	Adaptive Planning – Deployment Management	15
Sustainment Estimation	Adaptive Planning – Deployment Management	19
Transportation Management	Adaptive Planning – Deployment Management	18
Deployment Data	Adaptive Planning – Deployment Management	15
Strategic Guidance	Adaptive Planning – Employment Management	8, 20, 22
Concept, COA, and Effects Development	Adaptive Planning – Employment Management	7, 19
Plan Development and Refinement	Adaptive Planning – Employment Management	20
Employment Plan Data	Adaptive Planning – Employment Management	20
Employment Execution	Adaptive Planning – Execution Management	5
Deployment and Distribution Visibility	Adaptive Planning – Execution Management	15, 16,17
Joint Force Synchronization	Adaptive Planning – Execution Management	1
User Management	C2 Cross Functional	N/A
Analysis and Reporting	C2 Cross Functional	N/A
Redirection	C2 Cross Functional	N/A
Geospatial Rendering	C2 Cross Functional	N/A
Orchestration	C2 Cross Functional	N/A
C2 Collaboration	C2 Cross Functional	N/A
C2 Messaging CM	C2 Cross Functional	N/A
Air Task Order Data	Force Employment Air/Space Ops	2
Air Space Management Data	Force Employment Air/Space Ops	2
Air Mission Planning Data	Force Employment Air/Space Ops	2
Army Fires Data	Force Employment Ground Ops	2
Army Maneuver Data	Force Employment Ground Ops	2
Missile Defense and Warning	Force Projection	1, 6
Capability Based Force Options	Force Projection / Force Visibility - Capability Visibility	10, 18
Force Location and Availability Data	Force Projection / Force Visibility - Capability Visibility	10, 14
Force Apportionment Data	Force Projection / Force Visibility - Capability Visibility	10, 13

⁶ Acquisition Strategy

UNCLASSIFIED

Capability Module	Mission Area from CDD	CDP Reference
Force Structure Management	Force Projection / Force Visibility – Force Structure	10, 14
Joint Force Structure Data	Force Projection / Force Visibility – Force Structure	10, 14
Army Force Structure Data	Force Projection / Force Visibility – Force Structure	10, 14
Navy Force Structure Data	Force Projection / Force Visibility – Force Structure	10, 14
USAF Force Structure Data	Force Projection / Force Visibility – Force Structure	10, 14
USMC Force Structure Data	Force Projection / Force Visibility – Force Structure	10, 14
Readiness Assessment and Analysis	Force Projection / Force Visibility - Global Force Readiness	11
Joint Readiness Data	Force Projection / Force Visibility - Global Force Readiness	10, 12
Army Readiness Data	Force Projection / Force Visibility - Global Force Readiness	10, 12
Navy Readiness Data	Force Projection / Force Visibility - Global Force Readiness	10, 12
USAF Readiness Data	Force Projection / Force Visibility - Global Force Readiness	10, 12
Collection Management	Intel	9
Imagery Data	Intel	2
Global UDOP	Situational Awareness	1, 2, 3, 4, 5
Association Management	Situational Awareness	1, 2, 3, 5
Red Track Data	Situational Awareness	1, 3
Weather Data	Situational Awareness	2
Blue Force Ground Data	Situational Awareness	1
Blue Force Maritime Data	Situational Awareness	1
Blue Force Air Data	Situational Awareness	1

1.5 Piloting and Federated Development and Certification Environment (FDCE) Process Overview

1.5.1 Capability Provisioning Activities

Piloting is a means of developing an environment where Test and Evaluation (T&E) can be conducted in a realistic SOA environment. Each stage of the FDCE has a layering of certifications that will enable testing in different environments ranging from limited access to full operationally representative environments. Capability Provisioning Activities (CPAS) are a set of 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 Joint Combat Capability Developer (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.

To provide the speed and agility needed in both piloting and T&E, NECC relies on three types of piloting activity events: User Free Play (UFP) events, Capability Provisioning Events (CPEs) and Operational Concept Events (OCEs) (See paragraph 1.5.3 for more information on UFP, CPE, and OCEs).

1.5.2 Overview of the FDCE Environment

The FDCE is a certification/testing management tool for the CPAS process. It will provide the environment that will facilitate 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 Critical Operational Issue (COI) 1 (see Section 3.6). In addition, the Joint Program Management Office (JPMO), as the technical standard configuration control manager, will use the FDCE to provide 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 will track and display certifications for each piloting phase that will provide management of certifications in support of transition of piloting events as detailed in Figure 4. CMs can enter at different stages of the FDCE based on a maturity assessment, which will be conducted by the Joint System Team (JST). Once a CM has completed all of the certification and testing requirements for the Operation Piloting stage, a CM Assessment Report (CMAR) will be provided to the Milestone Decision Authority (MDA), or designee, to support a Limited Fielding decision. Besides test results, the CMAR will also document the results of all CM certification activities including Network Operations (NETOPS) and Net-Ready Key Performance Parameter (NR-KPP) certifications. Please see paragraph 3.5 for further information on CM Fielding. The “Environment” is referred to as federated to emphasize that it is not operated or used by a single organization. The FDCE neither owns nor operates the laboratories that contribute to the FDCE. However, the FDCE provides strict governance, administration, and day-to-day management for interconnections with those laboratories when participating in FDCE processes.

CPAS supports three major phases of testing within the lifecycle of a CM, (1) Definition, (2) Planning, and (3) Execution.

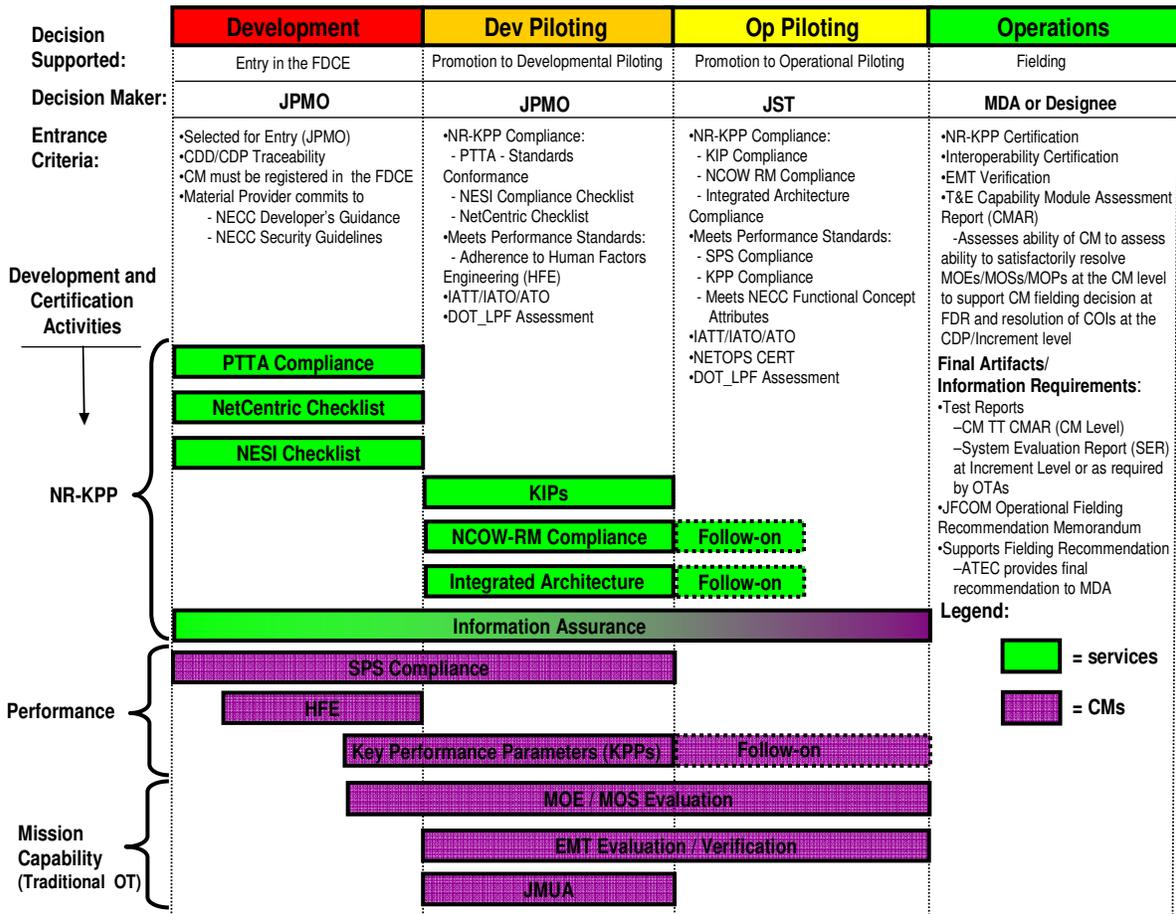


Figure 4: Certification Entrance Criteria for a CM and the Decision Makers

The Definition phase is where the CM is defined and entered into the FDCE with associated metadata. A Test, Evaluation, and Certification (TEC) Criteria is tailored for each CM by the materiel provider with the assistance of the T&E community. This key information is used to determine the feasibility and level of effort required to develop an operational capability. If after this process a candidate CM is selected for development it then enters the Planning phase.

The Planning phase is primarily concerned with associating the CM with development of a work package, initializing CPAS event scheduling and resourcing, and conducting an Upper Specification Limit (USL) assessment to scope the level of testing to determine whether a CM has met the entry stage criteria for the CPAS Implementation phase.

The CPAS Implementation phase consists of three stages used to mature a capability: (1) Development, (2) Developmental Piloting, and (3) Operational Piloting (as detailed in Figure 5). These stages progressively demonstrate that the tailored TEC Criteria necessary to field the capability on the operational GIG environment are satisfied. The development stage focuses on

capability development, standards conformance, debugging, and technical exploration. The developmental piloting stage enables early user feedback on operational utility, integration and net-readiness, and security evaluations. The operational piloting stage facilitates any remaining security, interoperability, supportability, and usability assessments required to support an implementation decision. When migrating a CM from one stage to the next, decision makers assess the capability's maturity relative to its tailored TEC Criteria and decide whether the capability should be moved to the next stage, remain in its current stage for rework, or be removed from the FDCE.

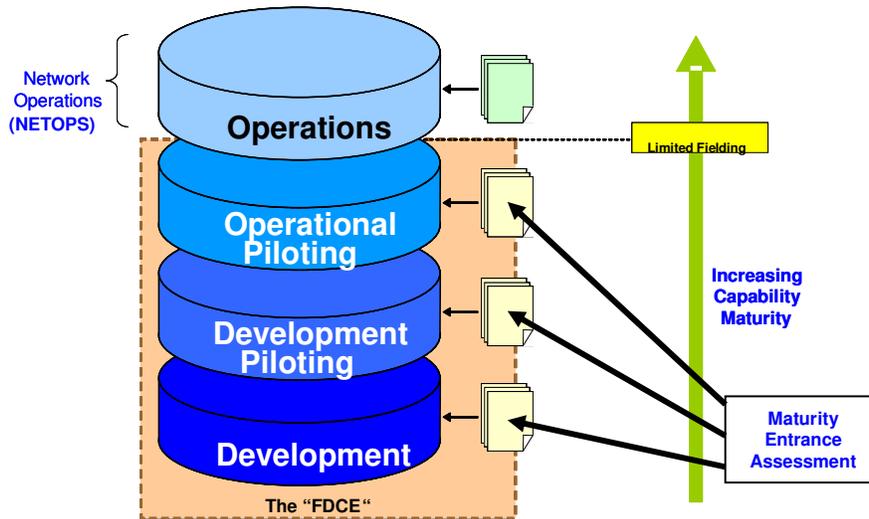


Figure 5: FDCE Stages

The FDCE is designed to speed up the process of certifying and accrediting C2 capabilities, not as a selection or elimination methodology, but by providing a distributed virtual environment that allows NECC stakeholders to remotely monitor, evaluate, and certify CMs as they advance through multiple maturity stages. A core set of tools will be made available through the FDCE portal. The JPMO is responsible for the licensing, maintenance, funding, Service Level Agreements (SLAs), personnel support, and help desk support for these tools. Additional tools will be hosted and maintained by organizations external to NECC. The organization providing the tool is responsible for the accreditation, SLA, personnel support, and help desk support for these tools. The JPMO is responsible for obtaining required licenses for Developmental Test and Evaluation (DT&E). The JPMO determines the types of tools required based on the needs of each of the Components. A tool list to support the FDCE is provided within the NECC FDCE portal.

1.5.2.1 FDCE Organizational Roles and Responsibilities

Each registered user will be assigned (based on their registration request) to one of four major roles. While the FDCE provides a common, consistent user interface with which to manage various CMs, users will have a unique set of actions depending on their role and where the CM resides in the FDCE lifecycle. The four major roles are addressed in the following sections.

1.5.2.1.1 *Warfighter/User Community*

The Warfighter/Operational user community performs an integral and ongoing part of CM evaluation. It is envisioned that the CPAS concept will make access to CMs as easy as today's internet browsing. Warfighters/users informally evaluate new capabilities as beta users, as well as participate in formal T&E events in operationally representative environments.

Warfighter/user organizations include the Combatant Commands (COCOM), JTFs, Joint Training Centers (JTCs), Numbered Fleets, Numbered Air Forces, Land Forces, Marine Corps, and Marine Expeditionary Force-level staffs. Warfighter involvement is requested through the JCCD to support operationally relevant Developmental Testing/Operational Testing (DT/OT). Through all applicable phases of testing (DT/OT) and for selected operationally oriented piloting activities, User Free Play (UFP), Capability Provisioning Events (CPE) and Operational Concept Events (OCE), the Warfighter will normally participate virtually via the FDCE from their respective government-issued workstation. This new approach will permit a broader range of Warfighter engagement and minimize the requirement for travel. Warfighters assigned to Service battle and development labs will also participate in evaluating CMs and providing timely, relevant, and thorough feedback during the certification processes.

1.5.2.1.2 Requirements and DOT_LPF and Policy Communities

The Requirements and Doctrine, Operations, Training, Leadership and Education, Personnel, and Facilities and Policy (DOT_LPF-P)⁷ communities participate in CPAS by prioritizing requirements for new capabilities that define how the services will be used operationally to support mission activities and capabilities. Requirements and DOT_LPF and Policy communities also participate through informal and formal evaluation processes to support continuous improvements of materiel solutions and to evolve and validate their portions of the solution. Ultimately, the Requirements, DOT_LPF and Policy communities will be able to operate the network services to explore the non-materiel impacts to the services and evaluate DOT_LPF and Policy solution sets. Requirement and DOT_LPF and Policy organizations include the Joint Staff, US Joint Forces Command (USJFCOM), Training and Doctrine Command (TRADOC), Naval Network Warfare Command (NETWARCOM), Global Cyberspace Integration Center, and Marine Corps Combat Development Command (MCCDC). Engagement with the NECC Requirements and DOT_LPF and Policy communities is coordinated through the USJFCOM-led JCCD process.

1.5.2.1.3 Materiel Provider/Sustainment Community

The Materiel 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 Defense Information Systems Agency (DISA), Air Force (AF) Electronic Systems Center (ESC), Marine Corps Systems Command (MCSC), Space and Naval Warfare Command (SPAWAR), and Communications-Electronics Life Cycle Management Command (CELCMC), as well as other capability providers such as National Geospatial-Intelligence Agency (NGA), Defense Intelligence Agency (DIA), and National Security Agency (NSA). COCOMs can also be materiel providers and support CM maturation.

1.5.2.1.4 Test, Evaluation, and Certification Community

⁷ JCCD Management Plan, URL: <https://gesportal.dod.mil/sites/necc/JCCD/default.aspx>

The TEC community (which includes policy makers, the test/evaluation communities, the security accreditation community, and the interoperability certification agent) participates in CPAS by establishing and applying the certification criteria for CMs as they go through the certification processes. The TEC community ensures that CMs are evaluated with enough rigor that they will not harm the GIG and meet the needs of the Warfighter. The T&E strategy is to assess each CM via a CMAR. This report will comment on the contribution that the respective CM satisfactorily supports the overall resolution of COIs at the CDP and increment levels. The T&E community tests and evaluates CMs to ensure they meet developmental and operational test objectives at each step in the maturation processes. The security accreditation community reviews CMs to ensure they meet IA/Security standards. Additional information can be found on the [NECC FDCE portal](#).⁸

1.5.3 Piloting Activities as Test Events

Piloting activities provide data collection opportunities and may serve as formal test events with appropriate Joint System Team (JST) or Capability Module Test Team (CM TT) involvement in the planning, execution, and reporting of the activity.

1.5.3.1 User Free Play (UFP)

UFP events are a type of piloting activity where individual Warfighters or requirements/doctrine providers submit feedback to the materiel provider on the CMs through largely unstructured activities by using the CM on the FDCE (similar to Beta Testing). This type of event may be planned, scheduled, and executed with very little lead-time and low overhead cost. The results captured in user surveys on the FDCE are usually qualitative in nature. Further information is available in the [UFP Standard Operating Procedure \(SOP\)](#)⁹. These events are primarily initiated to introduce emerging NECC capabilities to Warfighters early as alpha/beta users and provide capability in a less formal environment to provide Component Program Management Offices (CPMOs) and materiel developers with user feedback of capabilities being developed.

1.5.3.2 Capability Provisioning Events (CPE)

CPEs are piloting activities primarily focused on the T&E of new capabilities. These events are more narrowly focused than OCEs and require much less lead-time to prepare (weeks vs. months). However, this concept of a lightweight and agile process model is balanced by the rigor and repeatability evidenced by a flexible framework. This process is supported by planning, review, and assessment artifacts and by coordinated NECC Integration and Technology Piloting (I&TP) and/or a JST CPE Lead as appropriate. Further information is available in the [CPE SOP](#)¹⁰.

1.5.3.3 Operational Concept Events (OCE)

OCEs are piloting activities focused primarily on evaluating new operational concepts with a secondary objective of evaluating new C2 capabilities. These events allow materiel providers

⁸ 1 Aug 2007, URL: <https://fdce.sspl.disa.mil>

⁹ NECC UFP SOP

¹⁰ NECC CPE SOP

and test teams the opportunity to evaluate capabilities in the most realistic operational testing environment available. Results from OT conducted during an OCE are captured in a CMAR and are used to inform the decision to field the capabilities to an operational status. Planning, review, and assessment artifacts are coordinated by an OCE Lead designated by the NECC JPMO I&TP Branch and working in concert with the JST-designated CM TT. Further information is available in the [OCE SOP](#)¹¹.

1.6 System Threat Assessment

As the principal C2 capability for the DoD, NECC will likely be targeted for direct or indirect attacks as will associated Service, Agency, or Joint-provided data sources. Most threats are addressed in DIA published documents listed in Appendix C and will serve as the DIA-validated baseline for all threats. A complete discussion of the threat summary is maintained as a NECC CDD extension by the JCCD separately on the [USJFCOM portal](#). This Portal resource will be used by the T&E community to determine the scope of test required to address specific threats. Additional information will be provided in the TEMP Annex.

1.7 Key Performance Parameters¹²

NECC uses an evolutionary acquisition strategy in which capabilities are incrementally delivered in time-phased stages based on the maturation of key technologies as a trade-off for accelerated delivery and risk reduction. Key Performance Parameters (KPPs) are those attributes considered most essential for an effective military capability and capture the minimum operational effectiveness and suitability attributes needed to achieve the overall desired capabilities during the applicable increment.

The NECC program is currently baselined for requirements contained in the 07 June 2007 [CDD](#).¹³

The KPPs for the NECC program are:

- Shared Situational Awareness (SSA)
- Planning and Execution
- System Training
- Net-Ready

1.8 System KPPs as detailed in the CDD are summarized in Table 2.

¹¹ NECC OCE SOP

¹² Reference USJFCOM Capability Development Document, 07 June 2007, v1.0, URL: <https://gesportal.dod.mil/sites/necc/JCCD/default.aspx>

¹³ Reference USJFCOM Capability Development Document, 07 June 2007, v1.0, URL: <https://gesportal.dod.mil/sites/necc/JCCD/default.aspx>

UNCLASSIFIED

Table 2: Key Performance Parameters

Key Performance Parameter	Development Threshold	Development Objective
<p>KPP# 1 Shared Situational Awareness: Provide key and vital information via net-centric services on the disposition of friendly, enemy, neutral, and unknown forces to allow the effective exercise of Command and Control.</p>	<p>Conduct track management and/or be able to access for filter and display, 20,000 or more friendly, enemy, neutral and unknown tracks, at all sites responsible for providing track information to decision makers at all levels of Command and Control.</p>	<p>Provide user access to unlimited number of tracks and track information to decision makers at all levels of Command and Control.</p>
Key Performance Parameter	Development Threshold	Development Objective
<p>KPP#2 Planning and Execution: Provide warfighters at all levels of command and control contingency and crisis action planning, force deployment / sustainment / redeployment and mission execution capability in support of National Security Objectives and the Adaptive Planning and Execution process.</p> <p>Provide warfighters at all levels of command and control the ability to maintain force readiness and to report on the ability of forces, units, weapons, or equipment to deliver the outputs for which they were designed at the tactical, operational and strategic levels.</p>	<p>Conduct contingency and crisis action planning, force deployment, sustainment, redeployment, and mission execution activities via generation and modification of TPFDD files, query and production of reports, managing and maintaining user accounts and reference with TPFDD validation in support of</p> <p>OPORD/OPLAN for Crisis Action Planning in less than 96 hours and less than 12 hours for Contingency Planning from decision to execution resulting in a success rating of 80% and no warfighter incident reports containing significant or critical operational impact.</p> <p>Update readiness database records with maintenance activities to produce and verify accurate reports concerning forces, units, weapons, systems and equipment at the UIC (tactical) and OPLAN (operational) levels with a success rating of 90% and no warfighter incident reports containing significant or critical operational impact.</p>	<p>Conduct contingency and crisis action planning, force deployment, sustainment, redeployment, and mission execution activities via generation and modification of TPFDD files, query and production of reports, managing and maintaining user accounts and reference files simultaneously from multiple geographic locations with TPFDD validation in support of</p> <p>OPORD/OPLAN for Crisis Action Planning in less than 24 hours and less than 2 hours for Contingency Planning from decision to execution.</p> <p>Update readiness database records with maintenance activities via multiple applications to produce and verify accurate reports at multiple locations via multiple applications concerning forces, units, weapons, systems and equipment at the UIC (tactical) and OPLAN (operational) levels with a frequency of readiness database updates available throughout the systems in less than three (3) hours and</p>

UNCLASSIFIED

Key Performance Parameter	Development Threshold	Development Objective
		historical updates less than 24 hours.
<p>KPP#3 System Training: NECC shall provide dynamic, capabilities-based training support tools, either embedded or via the web, across the full range of integrated operations.</p>	<p>Training support tools must be assessed for ease of use and training support effectiveness as favorable by 70% of JS/C/S/A users in an operationally representative test environment.</p>	<p>Units must be capable of simultaneously conducting training exercises in Live, Virtual, and Constructive environments using modeling and simulation tools, either embedded or via the web.</p>
<p>KPP#4 Net Ready: Net-Ready: The system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.</p>	<p>The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate (IATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing* specified in the applicable joint and system integrated architecture views.</p> <p>* Data processing is defined as: The input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.</p>	<p>The system must fully support execution of all operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for Net-Centric military operations to include 1) DISR mandated GIG IT standards and profiles identified in the TV-1, 2) DISR mandated GIG KIPs, 3) NCOW RM Enterprise Services 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Approval to Operate (ATO) by the Designated Approval Authority (DAA), and 5) Operationally effective information exchanges; and mission critical performance and information assurance attributes, data correctness, data availability, and consistent data processing* specified in the applicable joint and system integrated architecture views.</p>

1.9 KSAs for Increment 1¹⁴

NECC KPPs are underpinned by supporting [Key System Attributes](#) (KSAs), performance attributes, and system requirements and characteristics as listed in Table 3. KPP and KSA attributes and requirements are written in a threshold/objective format per Joint Capability Integration Development System (JCIDS). As recent additions to JCIDS, KSAs are those system attributes considered most critical or essential for the design and sustainment of an effective military capability. NECC KSAs have been developed to provide clear linkage and relationships between NECC KPPs and more detailed NECC attributes and requirements.

Table 3: Key System Attributes

Key System Attribute	Development Threshold	Development Objective
<p>KSA# 1 Situational Awareness: NECC shall provide net-centric services capable of accessing, sharing (send and receive), collating, and displaying COP and CTP information at the source level of accuracy in a format tailored by the user for all physical domains, all components of the joint force, and special operations forces.</p> <p>Essential CTP and COP elements are:</p> <ul style="list-style-type: none"> - Location/status/intentions of friendly forces (current & planned) - Location/identity/status/intentions of hostile forces (current & projected) - Location/intentions of other forces/actors (neutral forces, NGOs, etc.) (current & projected) - Meteorological and Oceanographic (Current & forecast environmental conditions and their effects on weapons systems and operations) - Geospatial information - Political/diplomatic information (current & projected) - Media reports - Ensure appropriate access to data based on clearance validation and attributes associated with the data, <p>KSA# 1 Situational Awareness: (continued)</p> <p>users, processes, or environment</p> <ul style="list-style-type: none"> - Location status of medical, humanitarian assistance, and terrorist events 	<p>Integration of land, air/space, maritime/littoral & intelligence information into a Common Tactical Picture in support of the Common Operating Picture (COP).</p>	<p>Integration of land, air/space, maritime/littoral & intelligence information into a CTP in support of the COP.</p>
	<p>Display and update user requested COP information at the level of accuracy produced within 15 seconds of user request using standard message formats.</p>	<p>Display and update user requested COP information at the level of accuracy produced in 1.0 second or less of user request using standard & non-standard message formats.</p>
	<p>Provide 3D visualization of, amplification of and reference to source data for friendly, enemy, neutral, and unknown tracks, as well as ISR and logistics (deployment and distribution) data, in Near Real-Time (NRT), contained in a database capable of processing 20,000 or more tracks per user defined allocation table.</p>	<p>Provide 3D visualization of, amplification of and reference to source data for friendly, enemy, neutral, and unknown tracks, as well as ISR and logistics (deployment and distribution data) in NRT, contained in a database capable of processing an unlimited number tracks per user defined allocation table such that the shared situational awareness available to any NECC user regardless of the geographic viewing area, the scale of the geographic viewing area or type track being filtered is not limited by processing and storage capabilities of the system.</p>
<p>Subjective determination of degree to which a visual representation meets the requirements of 80% of the users, by user (1-5 scale: 1 fully, 5 unmet).</p>	<p>Subjective determination of degree to which a visual representation meets the requirements of 100% of the users, by user (1-5 scale: 1 fully, 5 unmet)</p>	

¹⁴ Reference USJFCOM Capabilities Development Document, 13 April 2007, v0.93

UNCLASSIFIED

Key System Attribute	Development Threshold	Development Objective
- Archived / historical COP data		
<p>KSA#2 Planning: (Planning & Execution in support of National Security Objectives) NECC shall provide the capability for distributed collaboration for the development and revision of plans and for plans execution.</p> <p>Essential elements are: Distributive and Collaborative Planning Synchronous and asynchronous collaboration services Readiness and Operational Capability Identification (sourcing) Movement, Sustainment and Tracking Reduce planning cycle time</p> <p>KSA#2 Planning: (continued)</p>	<p>Provide vertical and horizontal distributed collaboration for development of force generation, sustainment, and projection requirements from CDR level to JTF/JTF component level.</p>	<p>Provide vertical and horizontal collaboration for development of force generation, sustainment, and projection requirements from DoD level down to lowest deployable entity as defined by the Services.</p>
	<p>System shall be able to allow up to 1,500 simultaneous users per plan and up to 45,000 simultaneous users on the system.</p>	<p>System shall be able to allow up to 3,000 simultaneous users per plan and up to 75,000 simultaneous users on the system.</p>
	<p>System shall provide simultaneous access to all essential elements of collaborative services for all members of all the boards, centers, cells, and any other activities within a JTF HQ and between a JTF HQ, CDR, and the JTF Components.</p>	<p>System shall provide near real-time collaboration for all members of a JTF, including the edge tactical user, US Agencies, NGOs, Allied and Coalition Partners, DoD COEs, Joint Staff (JS), other Communities of Interest pertinent to the JTF, and between the other JTFs and CDRs.</p>
	<p>Synchronous collaboration services to include: Persistent workspaces for every board, center, cell, and other established activities Concurrent access to 150 sessions Non-persistent sessions for Ad Hoc meetings Concurrent access to 500 sessions Session participant metrics: 75% shall have 10, or fewer, participants 20% shall have 200, or fewer, participants 5% shall have 1000, or fewer, participants Scalability Sessions shall have the ability to scale (prioritize) and structure collaborative services in order to accommodate session users within system limitations Presence and Awareness All Users shall be able to view the current collaboration status of any other authorized</p>	<p>Provide asynchronous messaging services to include: Guaranteed delivery person-to-person and organizational messaging in support of record traffic environments A strong mechanism for message origin authentication, non-repudiation, and guaranteed delivery. Survivability alerts</p>

UNCLASSIFIED

Key System Attribute	Development Threshold	Development Objective
	<p>user to 98% accuracy</p> <p>Audio conferencing</p> <p>Chat/instant messaging</p> <p>Shared file space</p> <p>Video teleconferencing</p> <p>Shared whiteboard</p> <p>Asynchronous collaboration services for 4000 users to include:</p> <p>Person-to-person and organizational messaging (e.g., E-mail)</p> <p>Delivery of alerts</p> <p>Within 30 seconds</p> <p>Web Portal</p>	
	<p>Crisis Action Planning and Execution (after release of warning order)</p> <ul style="list-style-type: none"> - Support development and maintenance cycles for OPORD and associated products: < 96 hours - Time required to perform a readiness assessment: < 6 hours 	<p>Crisis Action Planning and Execution (after release of warning order)</p> <ul style="list-style-type: none"> - Support development and maintenance cycles for OPORD and associated products: < 24 hours - Time required to perform a readiness assessment: < 2 hours
	<p>Contingency Planning (upon receipt of a planning directive)</p> <ul style="list-style-type: none"> - Support development and maintenance cycle for OPLAN and associated products: < 12 months - Time required to perform a readiness assessment: < 48 hours 	<p>Contingency Planning (upon receipt of a planning directive)</p> <ul style="list-style-type: none"> - Support development and maintenance cycle for OPLAN and associated products: < 2 months - Time required to perform a readiness assessment: < 24 hours
	<p>Total Force Visibility</p> <p>Changes to current readiness data/information are visible globally within 2 hours of input.</p> <p>Track inventory readiness, availability, and apportionment down to the individual level, and respond to queries within 10 minutes of initial request.</p> <p>Provide automatic notification of dual tasking within 5 minutes of force sourcing.</p>	<p>Total Force Visibility</p> <p>Changes to current readiness data/information are visible globally NRT of input.</p> <p>Provide continuous check for potential dual tasking during force sourcing process and provide immediate notification when and if it occurs.</p> <p>Continuous and uninterrupted Track to asset level visibility</p> <p>Provide continuous and uninterrupted Track to asset level visibility; globally track inventory, readiness, availability,</p>

UNCLASSIFIED

Key System Attribute	Development Threshold	Development Objective
		and apportionment of all forces down to the individual level; and respond to queries within 1 minute of initial request.
	<p>Track to asset level visibility</p> <p>User queries across disparate data sources will identify the authoritative data source.</p> <p>Reports or Queries will be delivered in less than 7 seconds from the time query is issued at 99.999% accuracy.</p>	<p>Track to asset level visibility</p> <p>User queries across disparate data sources will identify the authoritative data source.</p> <p>Reports or Queries will be delivered in less than 2 seconds from the time query is issued at 99.999% accuracy.</p>
<p>KSA#3 Training Support:</p> <p>NECC shall provide, either embedded or via the web, training support tools to facilitate effective individual and collective team, staff and unit training. Essential training elements to enable individual, collective, and conceptual training:</p> <ul style="list-style-type: none"> - Designed in “ease of use” to minimize the need for extensive use of mobile training teams and resident schools to achieve individual and collective proficiency with NECC tools -Alert/notification of new training provided with new spiral capability - Web-based Training - Web-based transfer -Capability to support distributed exercises -Embedded Modeling and Simulation capability - Learning Management System for training managers 	<p>Ease of use and training support effectiveness must be assessed as meeting current IT industry benchmarks for ease of use, the current Joint National Training Capability (JNTC) construct and supporting Joint Training Functional Construct (JTFC) attributes and metrics.</p> <ul style="list-style-type: none"> - Help tools, diagnostic proficiency assessment tools, and training management tools must be embedded or available via the web to facilitate assessment and tracking of individual and collective proficiency. - Training tools must be available via the web - Training and remedial, on-demand support must be web transferable - Must have alerts to notify training managers of training updates and new capability. <p>Individual:</p> <ul style="list-style-type: none"> - 70% of functional users (JS/C/S/A) judge NECC training capability as favorable in a standard Operational Test environment - 70% of Systems Administrators judge NECC training capability as favorable in a standard Operational Test environment <p>Collective:</p> <ul style="list-style-type: none"> - Individuals and or units must be able to conduct training on operational systems without affecting real world picture/data. <p>Conceptual:</p> <ul style="list-style-type: none"> - Supports the learning and training attributes of Training Transformation (T2) as defined by Joint Knowledge Development and Distribution Capability (JKDDC), JNTC and Joint Assessment and 	<p>Conceptual:</p> <ul style="list-style-type: none"> - Meets all T2 standards of and is fully integrated with JKDDC and JNTC.

Key System Attribute	Development Threshold	Development Objective
	Enabling Capability (JAEC). - Supports JTFC attributes and metrics.	

1.10 Test, Evaluation, and Certification (TEC) Criteria

The NECC program uses the TEC Criteria as a means to define a ‘build-to-test checklist.’ This checklist consolidates CDD and CDP requirements, critical technical parameters, COIs, Measures of Effectiveness (MOEs), Measures of Suitability (MOSSs), and other factors that a materiel provider must satisfy prior to a fielding decision. These factors include all DOT_LPF and Policy and programmatic factors necessary for successful deployment and use of the CM. Criteria within the checklist are grouped by process stage and serve as a means to determine the maturity and readiness of a CM. A CM’s materiel provider is responsible for tailoring the TEC criteria which is then reviewed by the JST to ensure adequacy and testability.

Each element of the checklist is a discrete technical standard, net-ready, information assurance, performance, or MOEs and MOSs that can be tested to evaluate the degree to which a CM is compliant with established policies, regulations, and documented operational requirements. A master list of TEC Criteria available in the FDCE contains: the NECC profile, a core set of standards and requirements applicable to all capabilities, and additional common criteria applicable to most, but not all CMs available for selection and association with specific CMs.

The TEC Criteria for an individual CM captures the essential technical standards, net-ready, information assurance, performance, and operational requirements that must be satisfied in order to field a CM to the GIG. The CM TEC Criteria is composed of three parts:

1. NECC Profile. The development of TEC Criteria begins with the NECC profile. These are the technical standards required for a CM to operate in the SOA environment as well as some net-ready requirements. These criteria pertain to all CMs.
2. Common CM Specific Criteria from the FDCE Master List of Criteria. Additional common criteria found in the master list on the FDCE are added based upon recommendations from the JST. These criteria are fairly inclusive of the entire NECC CM family, pre-populated in the FDCE, and selectable via a wizard on the FDCE.
3. Unique CM Specific Criteria defined by the JST and CM TT. Additional TEC Criteria not found in the master list on the FDCE but identified as testable requirements by the JST and the respective CM TT after reviewing all applicable requirements documentation. Applicable categories include technical standards, net-ready, information assurance, performance, mission capability and Operational Test Agency (OTA) metrics. As with the master list, these added criteria will have an owner who is responsible for the description, requirement source, assignment to a piloting and test, evaluation event, test methodology, and test tool identification if applicable. The owner will also determine who will perform the test, who will validate or evaluate the results, and who is responsible for any applicable certification.

More information about the [FDCE and the TEC Criteria](#)¹⁵ can be found on the Defense Online (DOL) portal.

1.11 Measures of Effectiveness and Suitability

MOEs and MOSs for the increment level COIs are part of the planned System Development and Demonstration (SDD) activities and will be included in the TEMP for the NECC Milestone C.

1.12 Critical Technical Parameters/Service Performance Specifications

In the NECC program, the Critical Technical Parameters (CTPs) will be selected from the Service Performance Specifications (SPSs). SPSs will be measured for each CM and will be included in future TEMP Annexes to detail specific developmental and operational performance requirements to be tested at the appropriate time. SPSs are measurable system characteristics that, when achieved, allow the attainment of desired technical performance capabilities within a CM. They are not user requirements. Rather, they are technical measures derived from desired mission capabilities. Failure to achieve a critical technical parameter should be considered a reliable indicator that the capability is behind in the planned development schedule or will likely not satisfy the requirements of a CDP.

A CMs ability to fulfill the requirements of the CDP guiding its development is measured against the SPSs. Each CDP provides thresholds and objectives for development through evaluation of the standards conformance requirements identified for the CMs. CPAS events are opportunities to measure the integrity of the CM as it matures. For most SPSs, their identified thresholds should allow for growth towards the objective requirement as the CM progresses toward achieving the desired capabilities.

1.13 Risk Areas and Risk Mitigation

DoD risk management involves the major activities of risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking. Risk management for NECC incorporates these activities and bases them on DoD and industry best practices tailored to meet the needs of the NECC Acquisition process. The [NECC Risk Management Plan](#) (RMP)¹⁶ discusses the formal, forward-looking, and continuous risk management process that controls risks through risk mitigation planning and implementation rather than on risk avoidance, transfer, or assumption. The procedures outlined in the DoD Instruction (DoDI) 5000.2, "*Operation of the Defense Acquisition System*," and guidance set forth in the Risk Management Guide for DoD Acquisitions, Sixth Edition serve as the basis for this approach.

For T&E the NECC program will use three instances of Test and Evaluation Risk Assessments (TERA). The first instance of TERA will occur at the JST level by conducting risk assessments at the CM level IAW Director of Operational Test & Evaluation (DOT&E) memorandum *Guidelines for Conducting Operational Test and Evaluation (OT&E) for Software Intensive*

¹⁵ 1 Aug 2007, URL: <https://fdce.sspl.disa.mil>

¹⁶ 31 July 2007, URL: https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

*System Increments*¹⁷. The results of this assessment will propose to the JST and DOT&E an adequate level of OT to mitigate CM risk. The proposed level of OT for each CM will be documented in the TEMP Annex and will provide the foundation for all CM OT planning. The second type of risk assessment assesses the level of net-ready maturity for a specific CM. Software tools will be used to perform this assessment, and a JITC prototype NECC risk assessment tool is currently being evaluated for this purpose. The result of this assessment determines at which stage the CM will enter the FDCE process. Additional information is located in Section 3 of this Capstone TEMP and the [FDCE portal](#)¹⁸. A third area of risk and a key NECC CDD requirement is the transition of GCCS FoS capabilities to NECC without degradation in capabilities. The approach to this objective is contained in [GCCS FoS to NECC Functionality Transition Plan \(FTP\)](#)¹⁹. The implication for the NECC T&E Strategy is the need to explicitly ensure that CM test approaches incorporate appropriate test processes that meet this objective, and that these approaches are a prominent feature of TEMP annexes and Detailed Test Plans (DTPs).

2 INTEGRATED TEST PROGRAM SUMMARY

2.1 Scheduling

Figure 6 shows the planned NECC Integrated Test Program Increment 1 schedule with milestones and significant testing events noted. Program funding profiles are currently being reviewed. The approved funding profile will be provided following the Milestone B decision.

¹⁷ Office of the Secretary of Defense - Operational Test and Evaluation, 16 June 2003, Memorandum for Distribution, *Subject: Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments*.

¹⁸ 1 Aug 2007, URL: <https://fdce.sspl.disa.mil>

¹⁹ GCCS FoS to NECC Functionality Transition Plan, v1.0, 17 July 2007, https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

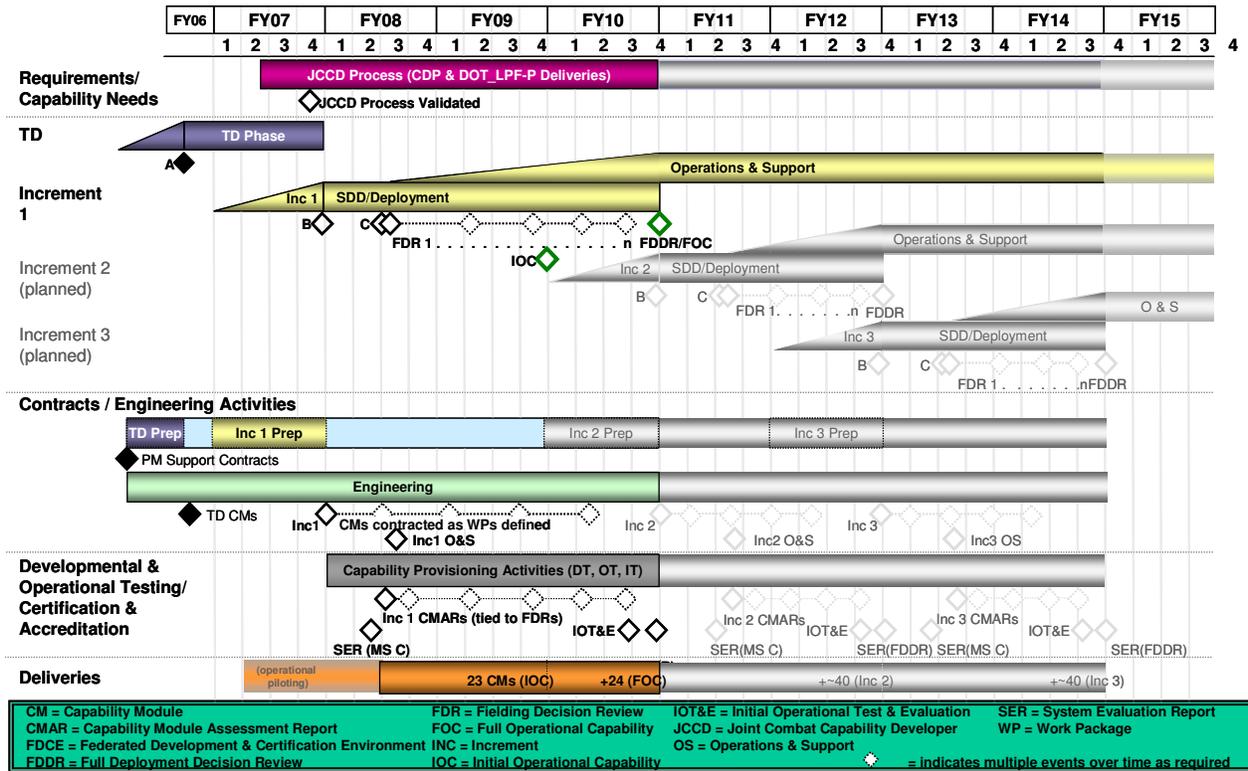


Figure 6: NECC Integrated Test Program Schedule

2.2 Management

The following organizations play key roles in the overall management, planning, and implementation for testing the NECC Increment 1 portfolio of capabilities.

2.2.1 NECC Test Teams

2.2.1.1 Joint System Team²⁰

The JST consists of representatives from the organizations listed below. JST core members will provide standing representation throughout the NECC program lifecycle. Participating organizations may vary as the program evolves. The JST directs the formation of CM TTs that produce test plans, test procedures, and execute specific tests or resolve test issues. The JST is Tri-Chaired by the lead OTA, the NECC JPMO representing the Joint Program Executive Officer (JPEO), and the USJFCOM JCCD. The JST consists of the following core members (who are polled by the tri-chairs on matters requiring a vote) and participating members (who provide unique expertise to the JST).

1. JST Core Members:
 - a. Operational Test Agencies

²⁰ NECC JST Charter July 2007

UNCLASSIFIED

- Army Test and Evaluation Command (ATEC) (Lead OTA)
 - Air Force Operational Test & Evaluation Center (AFOTEC)
 - Commander, Operational Test and Evaluation Force (COMOPTEVFOR)
 - Marine Corps Operational Test and Evaluation Activity (MCOTEA)
 - Joint Interoperability Test Command (JITC)
- b. JPEO/JPMO
- Army CPMO
 - Air Force CPMO
 - Navy CPMO
 - USMC CPMO
 - DISA CPMO
 - Information System Security Engineer (ISSE)
- c. USJFCOM Joint Capability Developer (JCD)
- JCCD, Lead Operational User
 - Joint Systems Integration Command (JSIC)
2. JST Participating Members:
- The participating members are non-voting members of the JST and provide subject matter expertise to the JST/CM TT body.
- a. Office of the Secretary of Defense (OSD)
- Director, Operational Test & Evaluation (DOT&E)
 - Under Secretary of Defense(Acquisition, Technology, and Logistics) OUSD(AT&L)
- b. Developmental Test Activities
- Air Force 46th Test Squadron (46TS)
 - Space and Naval Warfare Systems Center (SSC)
 - Marine Corps Systems Command (MARCORSYSCOM)
 - Army Developmental Test Command (DTC)
 - Joint Interoperability Test Command (JITC)
- c. Others
- US Strategic Command (USSTRATCOM) (DAA)
 - Joint Staff (J-6)

Specific JST roles and responsibilities include:

1. Develop and manage the T&E strategy and TEMP Annex for each CDP to support the requirements, acquisition, and sustainment strategies.
2. Recommend to the lead OTA the formation of CM TTs to address T&E data analysis, problem solving, test planning, test execution, and reporting.

3. Work with JCCD and NECC SE on the CDP to assist in the decomposition of requirements, mission threads, ensure testability of requirements, and define the appropriate test events and requirements.
4. Perform CDP/CM risk assessments and create the test concept for the System Evaluation Plan.
5. Participate in planning stages and help to conduct piloting events and exercises/experiments, as appropriate, to decide how the data produces from these events may be used for CM evaluation/assessment purpose.
6. Develop Additional Issues (AIs) and the supporting MOEs, MOSs, and Measures of Performance (MOPs).
7. Manage testing of the CM (and all of the associated CM TTs underneath).
8. Maintain master TEC Criteria (keeper of the process, which includes standard plan & report formats, deficiency report format, tools, etc.).
9. Provide inputs to the TEMP including coordinating resource requirements for all OTAs.

2.2.1.2 Integration and Technology Piloting Team (from [I&TP Concept of Operations \(CONOPS\)](#)²¹)

1. Participate in the planning, coordination, and implementation for all piloting events at the guidance of the JST.
2. Leverage testing opportunities from Services and COCOM exercises and experiments.
3. Participate as a Subject Matter Experts (SME) for the JST.

2.2.1.3 CM Test Team

The CM TT defines and carries out a detailed test plan for each CM that supports the TEMP Annexes for the associated CDP. The test team focuses on the specific CMs assigned. Test events may encompass one or multiple CMs. The test team membership includes an OT and DT lead. The team will leverage SMEs to include, but not limited to, IA certifiers and interoperability testers. Additional members may include USJFCOM-JSIC, Warfighters, NECC JPMO, Materiel Providers/CPMOs, DOT&E, and OUSD(AT&L) Defense Systems (DS)/SE/Assessment and Support (A&S). The CM TT roles and responsibilities include:

1. Develop DTP(s) required to support the T&E strategy outlined in the TEMP Annexes.
2. Integrate test vignettes, scenarios, scripts, etc. into CPAS events to support the JST-developed TEMP Annex.
3. Execute the DTP and collect data.
4. Collect data generated from I&TP lead CPAS events.
5. Analyze and provide to the JST authenticated Level 3 data.
6. Generate a CPE report for DT and a CMAR for OT.

²¹ 20 June 2007, URL: <https://gesportal.DOD.mil/sites/necc/integration/default.aspx>

2.2.1.4 Joint Interoperability Test Command

JITC provides SME for all matters affecting compliance with Joint Interoperability policies. JITC shall develop the NR-KPP Certification Test Methodology for NECC and certify TEC Criteria supporting the NR-KPP for each CM. JITC shall support the development of FDCE web pages and test report templates by gathering User Interface requirements from the TEC community.

2.2.2 *Assistant Secretary of Defense for Networks and Information Integration*

NECC is designated both a pre-Major Defense Acquisition Program (MDAP) and a pre-Major Automated Information System (MAIS). OUSD(AT&L) memorandum of 16 February 2007, assigns Acquisition Category (ACAT 1D) and delegates the MDA to the ASD(Networks and Integration Information (NII))/DoD Chief Information Officer (CIO). The MDA exercises acquisition decision authority over NECC development and implementation efforts. The MDA may delegate acquisition authority for milestones and decision reviews. The NECC JPEO and Joint Program Manager (JPM) provide programmatic and execution progress to the MDA through periodic reporting.

The Deputy Assistant Secretary of Defense (DASD) Command, Control, Communications (C3), Space and Spectrum (S&S) acts as the OSD Principal Staff Assistant (PSA) and works with USJFCOM, Joint Staff, and JPEO to address and resolve any issues relating to interoperability, standards compliance, security, net-centric attributes and data strategies, best practices identification, lessons learned adoption, program modifications, and protocol that are critical to the end-to-end operation of the GIG.

2.2.3 *Designated Approval Authority for Information Assurance, USSTRATCOM*

USSTRATCOM is the DAA for NECC. The DAA accredits NECC capabilities in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP). The DAA is responsible for enforcing the implementation of security policies and procedures in the NECC operational environment.

2.2.4 *Lead Component for the Net-Enabled Command Capability, DISA*

The DISA Component Acquisition Executive (CAE) provides component level oversight of the NECC program and serves as the Lead Acquisition Executive for the NECC program. Periodic program reviews with the DISA CAE ensure effective disciplined planning, program execution, and decision-making. The DISA CAE has the authority to nominate the Joint Program Executive Officer, designate the JPM, and ensure the JPMO workforce obtains the education, experience, and training requirements for Defense Acquisition Workforce Improvement Act (DAWIA) certification for senior positions.

2.2.5 *Joint Program Executive Office for the Net-Enabled Command Capability*

The JPEO has full execution year authority for all aspects of the NECC Acquisition program. This includes program cost, schedule, and performance baseline objectives and responsibility for all NECC capability development. The JPEO defines, via a Memorandum of Agreement (MOA) with each Service Component, the responsibility for specific implementation activities critical for implementation success within the Components.

In consultation with the Acquisition Executives of the Military Departments, the JPEO serves as chartering authority for all NECC CPMOs and establishes program-reporting requirements. To that end, the JPEO directs and resources the NECC CPMOs to design and develop NECC capabilities, within agreed performance, schedule, and cost constraints. The JPEO conducts periodic NECC program reviews to ensure NECC CPMOs are meeting approved baselines and other NECC program objectives. Figure 7 shows the JPEO Organization.

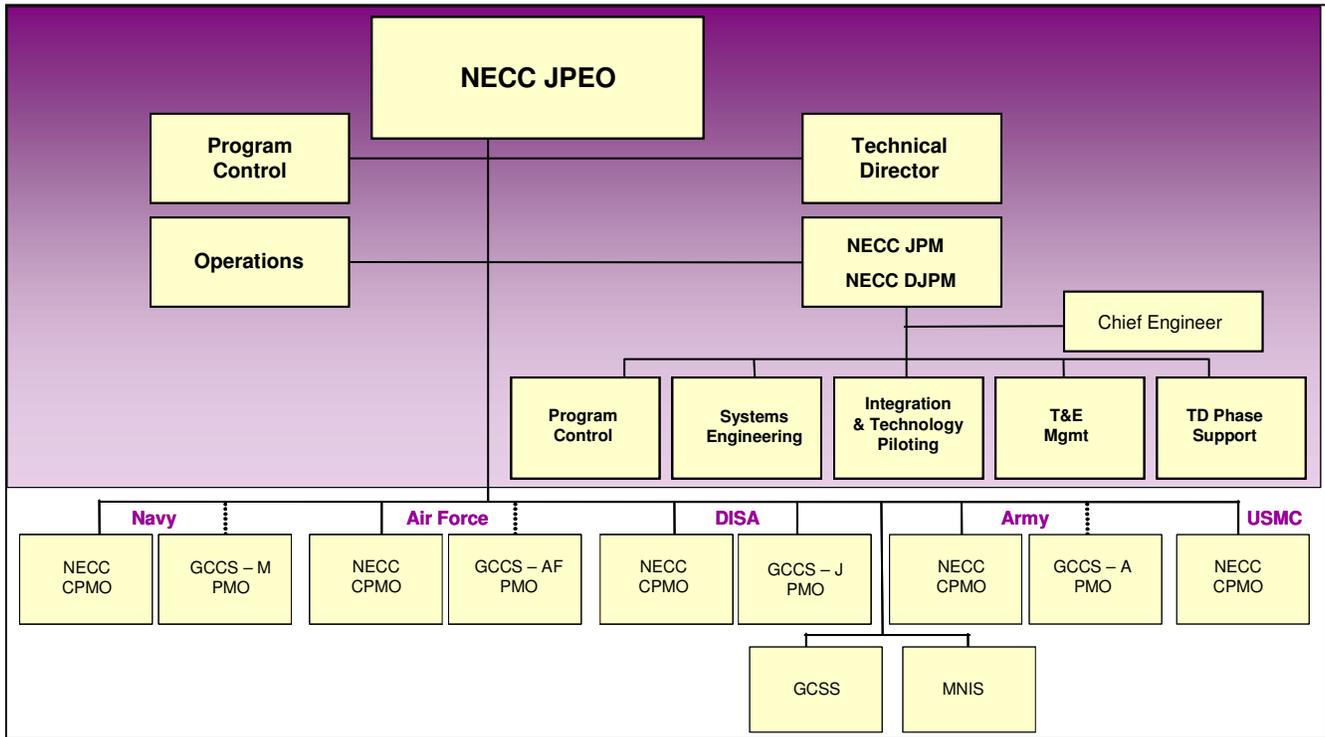


Figure 7: JPEO Organization

The JPEO is further responsible for establishing, publishing, and controlling the centralized systems engineering processes and standards for the NECC program as well as supporting the development of operationally effective and suitable NECC capabilities. The JPEO ensures compliance with NECC architecture, Net-Centric Data Standardization, Configuration Management, IA, standards management, T&E, and technology development strategies. A complete list of JPEO roles and responsibilities is outlined in the [NECC Terms of Reference \(TOR\)](#)²². Specific roles and responsibilities include:

1. Provides O-5/O-6 level (or civilian equivalent) representation to serve as Tri-Chair to the JST.
2. Provides all appropriate support to ensure effective Integrated Test and Evaluation (IT&E) execution of the specific roles and responsibilities of the NECC JPMO.
3. Participates with OSD(NII) as an acquisition streamlining pilot program for exploring changes to the acquisition process.

²² <https://gesportal.DOD.mil/sites/necc/integration/default.aspx>

4. Assists in adjudication of IT&E issues that rise to the “GO” Level.

2.2.6 Joint Program Management Office (JPMO) for NECC

The JPMO serves as a Tri-chair for the JST and manages the development of the NECC programmatic strategy, architecture, systems engineering, and migration plans to move C2 systems from current architectures to a net-enabled capability. The NECC JPMO is responsible for articulating program objectives and status to the NECC Communities of Interest. The JPMO retains ownership of this NECC Capstone TEMP as well as subsequent TEMP Annexes. 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 prioritizes competing programmatic activities through strategic decision-making processes. The JPMO coordinates and collaborates with the CPMOs to produce NECC capabilities. Specific roles and responsibilities include:

1. Represents JPEO on the JST.
2. Functions as funding source for all JST actions, to include JST IT&E activities.
3. Establishes a deficiency reporting and tracking system for the NECC program.
4. Prioritizes, certifies, and resolves deficiencies submitted during DT&E, IT&E, and dedicated Operational Test & Evaluation (OT&E).
5. Coordinates with the NSA Information Assurance Directorate (IAD) those program objectives that require IA certification or support to enable their timely development and evaluation.
6. Provides coordination between the JST and the NECC Configuration Control Board (CCB) to review specific IT&E issues that may arise from CM product design changes and recommend CM fixes/Engineering Change Proposals (ECPs).
7. Funds and oversees the FDCE Verification and Validation (V&V) requirements.
8. Funds and oversees NECC Modeling and Simulation (M&S) V&V Accreditation (VV&A) effort.

2.2.7 Component Program Management Office

Each Service and the DISA provides a CPMO to coordinate component-unique support to the JPMO for the NECC program. Specific JST responsibilities for all CPMOs are listed in the bullets below:

1. Participates on the CM TT for applicable CMs.
2. Leads DT effort on Component-assigned CMs and supports operational/combined testing, when applicable.
3. As a member of the JST and CM TT, designs, plans, programs, coordinates, and executes a viable CM IT&E program.

UNCLASSIFIED

4. Assists in developing and tailoring the TEC for assigned CMs.
5. Ensures CM work-related workspaces in the FDCE are complete and maintained for assigned CMs.
6. Coordinates all CM TT actions with the materiel providers of the assigned CMs.
7. Assists in developing and maintaining the NECC T&E documentation.
8. Coordinates the T&E strategy for each CM with the JST.
9. Facilitates CM TT 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.
10. Provides status report to the JST on progress/results of DT.
11. Participate in coordinating CPE events for assigned.
12. Coordinates with the JPMO to fund IA validation/certification activities through the work packages.

2.2.8 U.S. Joint Forces Command

Joint Requirements Oversight Council Memorandum (JROCM) 167-03, dated 22 Aug 03, assigned oversight of NECC requirements/ capabilities and execution of non-KPP authority to USJFCOM. The JC2 Analysis of Alternatives (AoA) recommended the establishment of the JCCD and associated processes to facilitate cooperation with the JPEO to ensure complete DOT_LPF and Policy are in place to support the Departments' Joint C2 mission.

As part of the Department's capability portfolio management test case, USJFCOM as the JC2 Capability Portfolio Manager exercises CDD oversight and execution approval authority for non-KPP requirements/capability needs adjustment for selected C2 portfolio programs to facilitate rapid and flexible capability development. The JCD (USJFCOM J8) as the execution arm of the C2 CPM and the Command and Control Capabilities Integration Board (C2CIB): identifies opportunities to improve Joint interoperability and streamline acquisition; manages portfolio visibility of JC2 capabilities focusing on the strategic-to-tactical needs of the JFC; orchestrates the development and delivery of JC2 capabilities to meet the Warfighter needs; and provides oversight and guidance as needed to support interoperability, integrated architectures, and data objectives. This provides the Component Program Manager (CPM) with the flexibility and authority necessary to rapidly identify and provide adjustments to spur timely capability development to meet Warfighter Joint C2 mission needs. USJFCOM JCD will provide a Operational Fielding Recommendation Memorandum for each CM to the MDA that provides recommendations for fielding based on operational and DOT_LPF and Policy considerations.

To fulfill NECC operational sponsor and requirements lead responsibilities, USJFCOM established the JCCD organization. The JCCD coordinates with the Operational community and oversees NECC's capability requirements. The JCCD representative represents USJFCOM and serves as a member of the JST Tri-chair. Specific roles and responsibilities include:

1. Provides O-5/O-6 level (or civilian equivalent) representation to serve as Tri-Chair to the JST.
2. Participates in resolving issues relevant to the JST.

UNCLASSIFIED

3. Provides subject matter expertise to the JST on matters concerning compliance with Joint operational requirements.
4. Prepares Joint COIs with Lead OTA and Component OTAs and ensures COIs are documented in the TEMP Annexes and System Evaluation Plan associated with each CDP.
5. Provides input to selected JST reports to generate CDP summary test reports.
6. Develops, coordinates, and provides JCD independent fielding recommendations for NECC CMs.
7. Coordinates with CCDRs, Services and Agencies to support JST validated requirements for Warfighter engagement throughout the CPAS process.
8. Monitors CMs through the Development, Developmental Piloting, and Operational Piloting phases.
9. Provides input to the TEMP, TEMP Annex, and other IT&E documentation.

USJFCOM, J-8, has assigned JSIC as the JCCD action arm to support the execution of the NECC Test and Evaluation program. Specific roles and responsibilities include:

1. Ensures Joint context and operational requirements are incorporated during each phase of testing.
2. Ensures DOTMLPF-P solutions are integrated and synchronized into test objectives and assessed during test events.
3. Supports all OTA conduct Joint Capability and Joint Interoperability Assessments IAW CJCSI 6212.01D and DoDI 4630.8, to ensure Joint Warfighter needs are met.
4. Supports the JST in the execution on the NECC IT&E program.
5. Provides inputs to JST members relevant to the TEMP development, Test, Evaluation and Certification Criteria (TECC), and CPE.
6. Monitors CMs as they progress through the Development, Developmental Piloting, and Operational Piloting phases as they move toward graduation.
7. Assists in reviewing JST detailed test plans and results.
8. Supports JST risk assessment of capability modules.
9. Identifies Joint/Coalition compatibility issues between NECC and legacy capabilities.
10. Ensures CMs, NCES, and other interdependencies are assessed to ensure Joint Warfighter operational capabilities are fielded.
11. Coordinates with DT/OT Leads for Warfighter participation and validates need for specific Warfighters in support of test team activities.
12. Represents the JCCD as a member of the deficiency review process.
13. Assists the JST to validate the Operational Mission Threads (OMT) (Joint integrated architecture) and Joint context (scenarios) used to support Joint operational objectives.

2.2.9 Director, Joint Staff

1. Facilitates the capabilities development process and entry into the JCIDS process.
2. Works with the ASD(NII)/DoD CIO, JPEO, the Services, and DISA to address issues relating to the requirements and operational effectiveness and operational suitability of the NECC program, to include the JCCD process.

2.2.10 Director of Operational Test & Evaluation

1. Advises the JST on all matters affecting compliance with DOT&E policies.
2. Provides procedural insights including assistance with identifying and resolving incongruent processes and expediting documentation review and approval.
3. Participates in and provide concurrence with recommendations from Risk Analysis / Level of Test (RALOT) reviews.
4. Approves the TEMP and TEMP Annexes.
5. Approves Operational Test Plans/Detailed Test Plans (or equivalent) for operational tests (or provisioning activities considered as equivalent to operational tests).
6. Provides operational test oversight including participating in test readiness reviews; observing test events; participating in data processes (authentication, scoring, review, and evaluation); and providing independent evaluations and reports.
7. Participates in the review process for reports and plans submitted to the JST.
8. Consults with the Tri-Chairs to facilitate resolution of issues arising within the JST.

2.2.11 OUSD(AT&L) System Engineering/Assessment and Support DT&E

1. Advises the JST on all matters affecting compliance with USD (AT&L) policies.
2. Assists in identifying and resolving incongruent processes and requirements.
3. Expedites OUSD(AT&L) review and approval of documentation.
4. Reviews the NECC TEMP and TEMP Annexes.

2.2.12 Operational Test Agencies

The OTAs include the ATEC as the lead OTA, supported by AFOTEC, MCOTEA, US Navy Commander, Operational Test and Evaluation Force, and JITC.

1. Responsible for all NECC operational test events assigned by JST, which may include Operational Assessments (OAs) and/or OT&E.
2. Participate with the JPMO in planning and coordinating CPAS events in accordance with the TEMP, TEMP Annexes and CM-specific Test Plans/Concepts.
3. Responsible for the development and submission of TEMP inputs, CMAR, and System Evaluation Reports (SER).
4. Participates as members of the JST and CM TTs.

2.2.12.1 Army Test and Evaluation Command²³

1. Serves as the lead OTA for NECC.
2. Provides O-5/O-6 level (or civilian equivalent) representation to serve as Tri-Chair to the JST.
3. Designates an OT lead for each CM TT.
4. Assists JPMO in development of the TEMP and TEMP Annexes by providing input through the Lead OTA.
5. Provides input required to develop the TEMP Annex for each NECC CDP.
6. Serves as OT Lead for CMs as agreed to by the supporting OTA and ATEC.
7. Supports other OTAs in the IT&E of their CMs.
8. Assists the JST in executing the NECC IT&E program by ensuring all Component-specific requirements are incorporated during each phase of testing.
9. Evaluates the operational effectiveness and suitability of NECC capabilities.
10. Exercises operational control and test management authority for Component-specific CM TTs in accordance with specific NECC or Component directives.
11. Designates a primary and alternate JST representative to provide expertise to the JST on matters affecting compliance with OT&E policies.
12. Reviews DT plans, reports and relevant documentation for each CM.
13. Monitors CMs through the development and developmental piloting phases.
14. Leverages DT to minimize redundancy and adequately scope the operational testing.
15. Drafts, publishes, and coordinates operational test plans, reports, data management plan IAW the JST standardized format, as appropriate.
16. Prepares an independent operational evaluation report IAW Component directives.
17. Provides Component-unique resource requirements, test resource requirements, user requirements, COIs, test objectives, measures of effectiveness, performance, and suitability (MOE/MOP/MOS) to the JST.
18. Provides CM test plans and reports to support evaluation of COIs at CDP and increment level.
19. Applies risk management at each CM or group of CMs to determine level of OT involvement, test to system, and Component-unique requirements.
20. Assists in the preparation and coordination of the deficiency reporting process.
21. Conducts Component characterization and scoring for Reliability, Availability, and Maintainability (RAM) parameters during Component-specific testing, and provides results.

²³ NECC T&E Lead OTA designation 12 Jan 2007.

UNCLASSIFIED

22. Establishes and chairs a joint reliability scoring team to assess test-incident mission impact and causality in support of a consolidated RAM evaluation (designated OT Lead for CM).
23. Provides comments/recommendations in the development of the TECC, as well as CPE.
24. Resolves issues as lead OTA, or elevates to the JST Tri-Chairs for action.
25. Exercises operational control or test management authority over CM TT in accordance with the JST charter.
26. Provides OTA member to the deficiency review process, if acting as CM TT OT Lead.
27. Consolidates test resource requirements by integrating test objectives and parameters for OT events.
28. Conducts necessary Component-level operational tests.
29. Reviews risk assessment for each CM, each CDP and each increment to determine level of OT involvement, and tests to system and Component-unique requirements.
30. Provides overall IT&E expertise to NECC program management.
31. Supports JPMO IT&E funding baseline efforts by providing timely OT funding requests and OT expenditure reports.
32. Acts as Data and Test Documentation Manager for OT test plans and reports.
33. Provides administrative services to the JST.
34. Provides funding requirements to JPMO for NECC JST and OT events.
35. Coordinates with the JCCD to jointly develop COIs for each CDP.

2.2.12.2 Supporting Operational Test Agencies

1. Provide appropriate representatives to the JST.
2. Assist JPMO in development of the TEMP, and TEMP Annexes by providing input through the lead OTA.
3. Provide input required to develop the SEP/TEMP Annex for each NECC CDP.
4. Serve as OT Lead for CMs as agreed to by the supporting OTA and ATEC.
5. Support other OTAs in the IT&E of their CMs.
6. Assists the JST in executing the NECC IT&E program by ensuring all Component-specific requirements are incorporated during each phase of testing.
7. Evaluate the operational effectiveness and suitability of the NECC system.
8. Exercise operational control and test management authority for Component-specific CM TTs in accordance with specific NECC or Component directives.
9. Designate a primary and alternate JST representative to provide expertise to the JST on matters affecting compliance with OT&E policies.
10. Review DT plans, reports and relevant documentation for each CM.
11. Monitor CMs through the development and developmental piloting phases.

UNCLASSIFIED

12. Leverage DT to minimize redundancy and adequately scope the operational testing.
13. Draft, publish, and coordinate operational test plans, reports, and data management plans IAW the JST standardized format.
14. Prepare an independent operational evaluation report IAW Component directives.
15. Provide Component-unique resource requirements; test resource requirements; user requirements, COIs; test objectives; and measures of effectiveness, performance and suitability (MOE/MOP/MOS) to the JST.
16. Provide CM test plans and reports to support evaluation of COIs at CDP and increment level.
17. Assist ATEC as lead OTA with implementation of RALOT processes at the CDP level for all CMs and with the development of CM operational test concepts.
18. Assist in the preparation and coordination of the deficiency reporting system.
19. Conduct Component -only characterization and scoring board for RAM parameters during Component -specific testing, and provides results.
20. Establish and chair a Joint reliability scoring team to assess test-incident mission impact and causality in support of a consolidated RAM evaluation (designated OT Lead for CM).
21. Provide comments/recommendations in the development of the TECC, as well as CPE.
22. Raise issues to the Lead OTA to resolve, or elevate to the JST Tri-Chairs for action.
23. Exercise operational control or test management authority over CM TTs in accordance with the JST charter.
24. Provide OTA member to the deficiency review process, if acting as CM OT Lead.
25. Consolidate test resource requirements by integrating test objectives and parameters for OT events.
26. Conduct necessary Component-level operational tests.
27. Review risk assessment for each CM, each CDP, and each increment to determine level of OT involvement, and test to system and Component-unique requirements.
28. Provide overall IT&E expertise to NECC program management.
29. Support JPMO IT&E funding baseline efforts by providing timely OT funding requests and OT expenditure reports IAW Section 8.0 of the [JST Charter](#).²⁴
30. Provide the NECC NR-KPP assessment/certification IAW CJCSI 6212.01D, DoDD 4630.5, and DoDI 4630.8 (JITC only).
31. Conduct joint interoperability certification for Command, Control, Communications, and Intelligence (C3I) systems and equipment that interface with or integrate into the Defense Information Infrastructure (DII) and the C3I structure of the DoD (JITC).

²⁴ 1 Aug 2007, URL:
https://gesportal.dod.mil/sites/necc/TE/TE%20WIPT/CTF%20Tiger%20Team/Shared%20Documents/JST%20Charter%20NECC_Ver%201.0b_Signed_30Jul07.pdf

32. Provide standardized test procedures for all OTAs to ensure NR-KPP compliance, to include IA requirements, using the agreed upon approach to IA assessment developed in close coordination with the NECC IA Working Group (JITC).

2.2.13 Developmental Test Agencies

The developmental test agencies include the Army DTC, SSC, Air Force 46TS, JITC, MARCORSYSCOM, and other commands as necessary.

1. Responsible for all NECC developmental test events assigned by the JST.
2. Participate with the JPMO in planning and coordinating CPAS events in accordance with the TEMP and CM-specific Test Plans/Concepts.
3. Responsible for the development and submission of CPE reports to the respective CPMO.
4. Participates as a SME for the JST.

2.2.14 Information System Security Engineer

1. Participates in resolving IA issues relevant to the JST.
2. Maintains appropriate IA certifications compliant with IA workforce requirements IAW DoD 8570.1-M.
3. Complies with the NSA Information Assurance Technical Framework (IATF) process (<http://www.iatf.net>).
4. Maintains situational awareness of IA for all capabilities throughout CPAS development for input into certification for the next development stage.
5. Serves as the IA representative, as designated by the JPMO to ensure all IA-specific requirements are incorporated during each phase of testing.
6. Supports materiel developers in the certification of their CMs.
7. Assists the JST in the execution of the NECC IT&E program.
8. Designates a primary and alternate representative to provide subject matter expertise to the JST on all matters affecting compliance with IA policies and governance.
9. Provides inputs to the JST for the TEMP development.
10. Reviews IA test plans, reports and relevant documentation for each CM.
11. Leverages IA testing to minimize redundancy and adequately scope required OT&E.
12. Monitors CM progress through the development and developmental piloting phases.
13. Provides status reports to the JST on progress/results of IA testing.
14. Drafts, publishes, and coordinates test plans, reports, data management plan IAW the JST standardized format, as appropriate.
15. Provides the JST with IA-unique resource requirements, test resource requirements, user requirements, test objectives, MOE/MOS to ensure the expected results meet the intent of the IA control.

16. Provides CM test plans and reports to support evaluation of COIs at CDP and increment level.
17. Applies risk management at each block upgrade to determine level of IA involvement, test to system, and Component-unique requirements.
18. Assists in the preparation and coordination of the deficiency reporting system.
19. Conducts risk analysis and mitigation determination and provides results for incorporation in the JST reports.
20. Provides comments/recommendations in the development of the TEC and CPEs.
21. Exercises IA test management authority over CM TT IAW the JST charter.
22. Coordinates with the Certification Authority (CA) for a certification recommendation and update of the NECC accreditation IAW the NECC C&A Process and DoDI 8510.bb, DoD Information Assurance Certification and Accreditation Process.

3 INTEGRATED TEST AND EVALUATION

The exit criteria stated for Milestone B primarily address the processes and technical maturity required for the NECC program to achieve success. There are no specific technical parameters identified in the exit criteria for T&E. As a result, the T&E community will support a risk assessment of the NECC process, including the FDCE, which will be provided at the M/S B decision. The MDA has been identified as ASN(NII) who will make the determination if the exit criteria have been met.

3.1 NECC Test Hierarchy Approach

The NECC program uses a two-tiered integrated test organizational approach. The JST is the first level of test hierarchy. The JST is an O-5/O-6 working level organization with representation from all test and certification stakeholders whose roles and responsibilities are outlined in the JST Charter and are identified in Section 2 of this Capstone TEMP. The second level of test hierarchy is the CM TT, composed of an OT Lead for operational test and a CPMO Lead for developmental test. The OT CM Lead is assigned by the lead OTA based upon recommendations from the JST. It is the responsibility of the CM TT to assess a specific CM or a combination of CMs based upon an established mission thread identified in the TEMP Annexes/System Evaluation Plan. The CM TT works closely with the I&TP team and the IA certifier and the JST to ensure synergy and efficiency.

3.2 Testing Governance

The decision authority to approve CMs advancement through the piloting maturity stages changes as the levels of maturity change. CM promotion from one stage to the next is accomplished electronically (i.e., E-Approval) via the FDCE. Regardless of the stage decision maker, the JPMO governs the conduct of Piloting events based on guidance from the JST. The JST will coordinate appropriate governance for piloting events that are considered formal test events. Developmental test events are conducted under the governance of the Component Program Management Offices and operational test events under the governance of the OTAs. This includes all types of piloting, including UFPs, CPEs, and OCEs. Figure 4 summarizes the

entrance criteria for each FDCE Stage. Further delineation of the entrance criteria will be accomplished within the JST. The NECC program will introduce a unique approach for fielding capabilities. This Capstone TEMP and future TEMP Annexes will support fielding of limited capabilities prior to the resolution of COIs at the increment level. The integrated T&E concepts support the assessment of MOEs and MOSs at the CM level and the resolution of effectiveness and suitability at the CDP and increment level.

3.3 Integrated Test and Evaluation Concepts

As discussed in Section 2, NECC uses an integrated T&E planning approach to offer the maximum amount of flexibility and necessary testing rigor to address the broad spectrum of capability maturity that will be acquired to fill the C2 needs of the Warfighter. NECC CMs will be tested via a series of CPAS that encompasses ALL levels and types of testing performed during the lifecycle of a capability. It allows the flexibility for the Program Office and Independent Test Agencies and Certifiers to tailor those tests into an appropriate comprehensive test approach for full spectrum integrated testing.

The T&E community works with the materiel provider and the JCCD to create, amend, and finalize an agreed-upon tailored CM TEC Criteria checklist for each capability. The TEC Criteria specifies in detail all applicable criteria and T&E methodologies. In tailoring the TEC Criteria, the T&E community prescribes test criteria and acceptable methods to perform the test to each performance standard. By defining accepted methodologies for automated testing and self-assessment, the T&E community may more easily leverage materiel providers' test results when executing independent test activities. It is imperative that T&E community members have the knowledge and skill required to negotiate the appropriate level of risk mitigation and to develop self-assessments, independent, and automated testing based on both the added value of the capability and the technology being used for implementation.

The NECC Integrated Test and Evaluation Strategy will use the DOT&E [*Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments*](#) to tailor CM OT events commensurate to the level of risk introduced by a CM. For CMs with low to moderate risk, OTAs will be able to reduce the scope of operational constraints and collect/analyze data from a DT event to assess MOEs and MOSs in a CMAR to support a CM fielding decision. The NECC T&E strategy, as detailed in Figure 8, integrates Developmental and Operational testing. This Capstone TEMP only covers Increment 1 requirements. A TEMP revision will be required for program milestones and each follow-on NECC increment. Within an increment, each CDP will be supported by a TEMP Annex which will follow the same format as the Capstone TEMP. Drafted by the JPMO, with assistance from the JST, the TEMP Annex addresses in a more detailed manner the resources and TEC methodology for evaluating a specific CDP and its associated CMs. ATEC will provide a System Evaluation Plan for each CDP that will provide the required T&E planning data necessary to populate the TEMP Annex. The overall NECC testing methodology is to leverage the engineered mission threads and business processes that establish their associated use cases. The JST community can use these artifacts to assist in the creation of Operational Mission Threads (OMTs) for their testing needs. As a result, the TEMP Annex will further decompose the Capstone TEMP COIs into CDP level COIs (AI) as appropriate to ensure alignment with OMTs to facilitate full requirements traceability from the operational level to the technical level. MOEs/MOSs will be derived from

these CDP level COIs/AIs and will be captured in the respective TEMP Annex. Each TEMP Annex, like this Capstone TEMP, is approved by DOT&E.

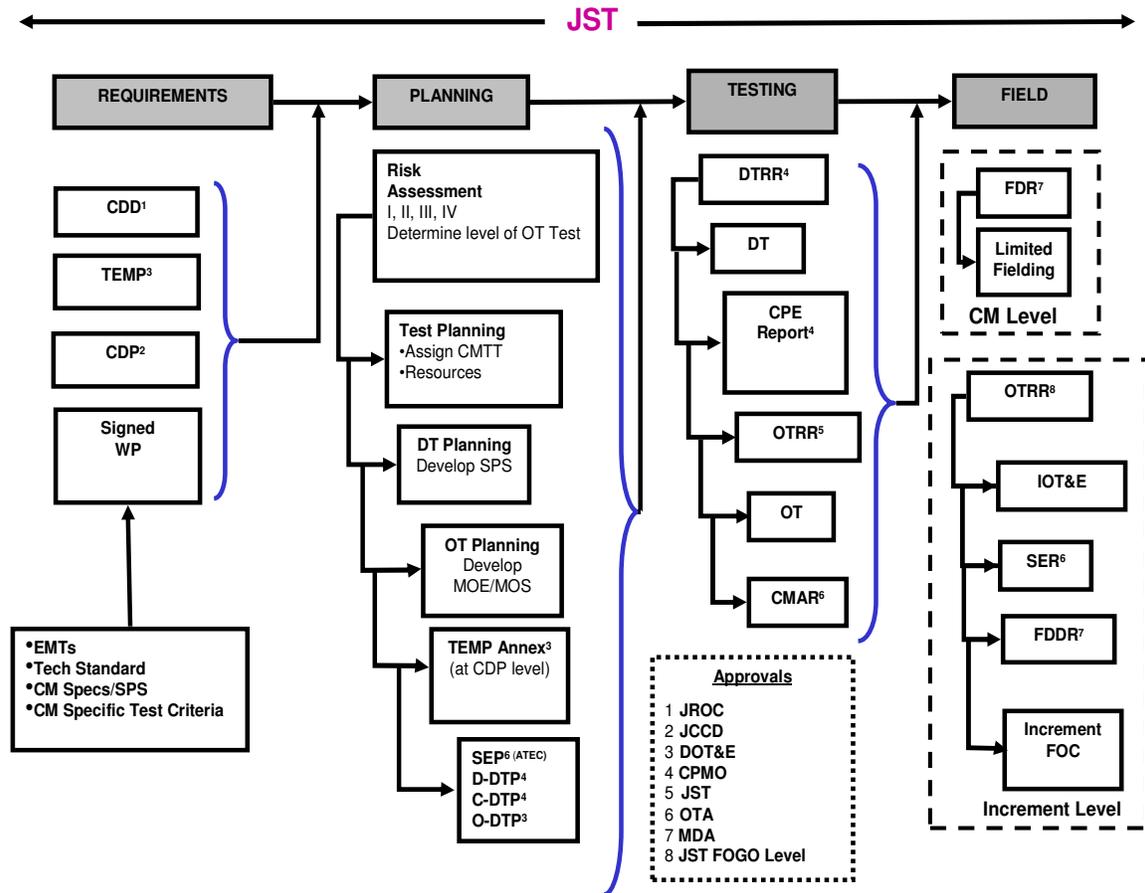


Figure 8: NECC T&E Strategy

3.3.1 Requirements Phase

The requirements phase is the initial step in the overall NECC T&E process. Prior to proceeding to the Test Planning phase, all documents referenced in Figure 8 will be finalized and approved by the appropriate authorities as specified in the figure text.

3.3.1.1 Capability Development Document

The Increment 1 CDD serves as the source operational requirements document for this Capstone TEMP. This CDD outlines the capability development strategy through which NECC will integrate existing and emerging C2 capabilities into a single, flexible, enterprise-based, architecture supporting the NMCS, JFC, Service and Functional Component Commanders, and subordinate Service commands. 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 JC2 architecture and capabilities-based implementation of NECC.

3.3.1.2 CDP Documents

The CDP is a tailored product of the JCCD capability needs process that provides the operational perspective, functional behavior, and performance detail to efficiently translate Warfighter requirements into acquisition and engineering terminology to streamline development, evaluation, and delivery of potential NECC DOT_LPF and Policy solutions to the Warfighter. CDPs are written at a high level without addressing the specific capabilities that make up a specific requirement. CDPs are written at a level of fidelity lying somewhere between the CDD (less detail) and the Capability Production Document (CPD) (more detail) which is not required for the NECC program. The CDP will include an operational context, refined requirements derived from the NECC CDD, and architecture views to support the capability requirements.

CDPs are not developed to address every individual capability requirement; rather, the JCCD may combine multiple NECC requirements and capabilities into a single CDP based on similarities in processes, functionalities, mission threads, linkages, interoperabilities, and created synergies. CDPs incrementally provide the materiel developer the fundamental information they need to rapidly produce and deliver operationally suitable and effective C2 capabilities. Each CDP contains a description of the desired capability, the conditions under which it must operate, the KPPs it must meet, and the high-level DoD Architectural Framework (DoDAF) with operational views to supplement that information. Each CDP will be supported by an Information Support Plan ISP Annex that will provide further detail with additional architectural products.

3.3.1.3 CM Work Packages (WPs)

NECC is based on an 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. CMs are a set of software and hardware that implement a set of operationally relevant, logically grouped services. A CM is the fundamental construct within NECC for providing operational capabilities. In general, NECC CMs will be implemented as a physically distributed set of Capability Nodes, which reside at NECC Sites. The NECC SE process provides guidelines for the nomination and creation of CMs. NECC services use, and are implemented in a manner consistent with and which interoperate with the CESs established by the NCES program.

A CM WP defines the activities necessary to develop/modify a CM and to support assessment of the capability through participation in one or more CPAS. It is comprised of one or more objectives, Engineered Mission Thread (EMT), Technical Standards, CM Specifications/SPS, and CM-specific TEC Criteria. The CM WP is assigned to a specific CPMO for development and integration. In some instances, where a logically related set of services will draw from more than one CPMO's base of existing capability, the JPMO may assign one CPMO as the "lead" for the CM, with other CPMOs in a support role.

3.3.2 *Planning Phase*

The entry point into the maturity stages is based on the initial assessment of maturity. This assessment of maturity is conducted after the materiel provider registers a CM into the FDCE and they are able to assert which TEC criteria have been satisfied based on any prior test and evaluation activities. The TEC community validates these assertions and develops the plans necessary to satisfy the remaining outstanding TEC criteria, based on Risk. Detailed Test Plans

(DTP) will be developed that outline the purpose, objective, scope, duration, limitations, modeling and simulation, and other resources necessary to satisfy the TEC criteria that are identified in the DTP.

Once all required Requirements Documents (CDD, CDP, and CM WPs) are approved and placed in the FDCE, the Test Planning phase will commence, as depicted in Figure 8. The JST, working closely with NECC I&TP representatives, will determine the association between CM TT membership and which CMs will be assigned to the test team.

3.3.2.1 CM Risk Assessments and Level of Test

A RALOT will be performed by the CM TT to determine the proper level of test required in order to adequately evaluate each candidate CM. This assessment will be performed as outlined in the DOT&E, *Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments*, 16 June 2003.

3.3.3 Test Plan Development

Once the risk assessment is complete to determine the level of operational test, the effort to develop the TEMP Annexes and subsequent detailed test plans commences. This phase includes the assignment of a CM TT and the identification of required resources (funding, tools, personnel, facilities, travel, etc.) needed to perform all levels and phases of testing that will be outlined in the System Evaluation Plan. It is important that these requirements are forwarded to the JPMO and JCCD for Warfighter support in a timely fashion to ensure that resources are properly funded and available prior to each testing phase.

3.3.3.1 Developmental Test Planning

During the Developmental Test Planning period the CM TT will identify those phases of developmental testing that are required to demonstrate the system's ability to meet specified systems performance requirements, and/or readiness to proceed to Operational Testing. As appropriate, the CM TT will integrate work package SPSs into the System Evaluation Plan for testing during a pre-determined phase of DT testing. The CM TT will also be responsible for determining testing resource requirements and schedule requirements for each phase of DT testing to be included in respective TEMP Annexes.

3.3.3.2 Operational Test Planning

The foundation for all operational test planning and execution will be based upon the roles and responsibility's established in the JST charter. The scope of this effort will be determined from the risk assessments conducted on individual CMs to ensure adequate level of OT. The level of test determination and operational mission thread analysis for CDP CMs will provide the baseline to develop the OT concept for each CDP. The test concept will be the first step for OTA planners to develop the detailed strategy to coordinate the testing of multiple CMs to address COIs at the CDP level. This detailed strategy will be documented in both a TEMP Annex and the follow-on detailed test plan. The OTAs will be responsible for validating the CM schedule for OT, test resource requirements and CM entrance criteria for formal test events. The CM TT Lead OTA will be responsible for developing the Operational Detailed Test Plan (O-DTP). The O-DTP will be a CM-specific test plan with identified test methodology and data

collection plan for each individual CPE executed. Prior to commencing OT, the CPMO will provide evidence that the CM is ready for at an Operational Test Readiness Review (OTRR).

3.3.3.3 TEMP Annexes

The TEMP Annexes will serve as a CDP-level T&E document that will detail required T&E strategies/approaches intended to satisfy CDP level SPS and COIs/AIs. The TEMP Annexes will also address the strategies to assess all test criteria for CMs to support a limited CM fielding decision at a FDR. The TEMP Annexes further describes the CMs that will be developed to satisfy the requirements of the CDP with methodologies and evaluation criteria for an accurate assessment for measuring the quality of the CMs and evaluating the performance based results. The evaluation criteria are the tools that allow evaluators to determine the success or degree of success each CM (or group of CMs) has achieved. These plans include, at a minimum, items such as expected outcomes, measures, and linkages from capability to military mission areas, and factors/conditions of each measure. The TEMP Annexes will discuss the proposed methodology test events (including Information Assurance Red Team Assessments) and resource requirements for compliance with the DOT&E IA policy.

The core elements of the TEMP Annexes will be automated to the fullest extent possible. For example, certification checklists, database parent/child rollups, and analyses routines lend themselves to automation. Ultimately, a data display could be provided to populate a test database for use in developing emerging results briefings and final evaluation reports.

Once the JST has a completed, approved TEMP Annexes and tailored TEC Criteria, any collected, authenticated data can be automatically tagged for use by other testing disciplines (i.e., DT, OT, Interoperability, etc) to satisfy their needs as well.

The format of the TEMP Annexes will be very similar to a system-level TEMP and will capture all agreed upon DT/Contractor Testing (CT)/OT testing phases, CDP level CTP/COIs, and required testing resources. The final approval for the TEMP Annexes will be DOT&E.

3.3.3.4 Detailed Test Plans

Upon approval of the TEMP Annexes, the respective CM TT will be responsible for the development of a DTP. The DTP will detail the overall testing approach to include specific testing scenarios/test cases, data/integration dependencies, and other required resources needed to test a particular mission thread or threads. All data, regardless of the level collected, will be archived for potential use by all test disciplines. This will allow for a ‘collect once, use many’ approach to data analysis and evaluation. As stated above, the data will be linked to the TEC Criteria by the JST to indicate to the community why the data is relevant, how the data will be used to evaluate the CM across the testing lifecycle, and if the data is a unique requirement for a particular event. If CMs are built iteratively, this data will also be made available for future use in integration efforts by new CMs or for configuration management purposes during CM upgrades, supporting regression testing, and determination of maturity. The approval authority for each level of DTP, detailed in Figure 8, is as follows:

- **Developmental DTP**
 - Respective CPMO
- **Combined Testing DTP**

- Respective CPMO
- **Operational DTP**
 - DOT&E

3.3.4 Testing Phase

Following the CM risk assessments and test planning efforts of the Planning Phase, the test article CM or multiple CMs will undergo testing. This testing is based those TEC criteria that have not been satisfied through prior test and evaluation or validated by the TEC community and identified as an area of risk. Some TEC criteria related to IA or NR-KPP may be addressed in DT and/or OT. The distinction of DT or OT is not meant to be holistically DT or OT focused, but rather each phase should be looked at as combined to satisfy the TEC criteria in totality or to a level of acceptable risk.

The CM TT will work with the I&TP team to establish a suitable environment to satisfy the outstanding criteria, including the identification of nodes, tools, instrumentation, and modeling and simulation assets necessary to satisfy the TEC criteria listed as objectives in the DTP. For DTPs that require user participation, the CM TT will work with the JCCD to identify the appropriate cadre of users to participate in the various types of structured and unstructured events to satisfy the TEC criteria. The CM TT will participate in a readiness review (DTRR or OTRR) at the appropriate levels and with approval to proceed will execute the event. Data will be gathered by members of the CM TT and posted (or linked) to the FDCE. The CPMO will post planning and reporting artifacts to the FDCE for DT events, while the CM TT OT Lead will post artifacts to the FDCE for combined DT/OT and OT events. Those artifacts will be validated by the appropriate TEC entities or recommended to be readdressed in later test events.

A TEC, DOT&E, and JST operational test representatives will monitor testing at their discretion to ensure the CM TT execute all testing activities per the respective developmental/operational DTPs. The CM lead will plan and execute the test event to collect new data related to CM performance. The CM lead will also organize the collection of existing test data for independent analysis. The CM TT, in collaboration with the I&TP team, will develop the necessary test cases, test scripts, scenarios, or other testing tools needed to generate the data identified by the JST for evaluation. The CM TT may also work with other organizations like the Test Resource Management Center (TRMC) and the Joint Mission Environment Test Capability (JMETC) to identify operationally realistic test environments and use certified models and simulations to support the test execution. The JCCD, as part of the JST, will coordinate with the CM TT and I&TP to ensure identification and use of relevant Joint scenarios necessary for implementation of Joint context consistent with the CDP.

Where possible, the test scripts and cases will be available to the materiel providers to self-test the CMs and automatically provide the data to the responsible CM TT. This situation is most likely to occur for immature CMs, and best supports a test-fix-test cycle of development testing. The goal is for all test event plans and reports to be documented and stored within the FDCE, making them available and accessible from a single source to all communities of interest. Test events conducted in direct support of a major acquisition decision (MS C or Limited Fielding Decision) will have plans that are approved by the appropriate OSD oversight official (AT&L, DT&E, and/or DOT&E).

Not all test events will be able to provide data for every test discipline. The combined utility of test events will evolve along with the CM through the testing process. At the onset of a testing process, a considerable focus of effort will be on those events needed to confirm standards conformance, technical achievement, and maturity. During the Development phase, it is expected that the role of the CM TT will be to monitor and confirm the validity of data collected from ongoing I&TP events. As a CM matures into the Developmental Piloting and Operational Piloting, the role of the CM TT will become more active. Potential test events that are included in the planning of an Integrated Test Event are listed below, categorized by test discipline. These require no definition other than they are the basic, universally accepted test events used in acquisition testing today. Respective test execution phases/milestones are as follows:

3.3.4.1 Developmental Test Readiness Review

A Developmental Test Readiness Review (DTRR) will be required prior to any phase of Developmental Testing to assure that all entrance requirements are met prior to formal DT. The respective CPMO has overall decision to proceed to DT.

3.3.4.2 Developmental Testing

Developmental Testing will be conducted to assess the CMs maturity and readiness to progress to the next phase of testing. DT testing can be performed in either the developmental or the operational piloting FDCE stages and should be conducted in an operational representative environment prior to any phase of OT.

3.3.4.3 Operational Test Readiness Review (OTRR)

OTRRs are required prior to the conduct of dedicated OT. Test results from previous phases of developmental testing will be reviewed to assess the overall maturity and readiness of CM(s) to proceed to OT. At the CM level the OTRR will be chaired by the tri-chair membership of the JST for each OT testing phase to formally certify the CMs as ready for test. For Initial Operational Test and Evaluation (IOT&E) at the increment level a Tri-Chair consisting of the Component Acquisition Executive (CAE), JCD, and ATEC Commander will serve as the chairs for the OTRR certifying the increment ready for test.

3.3.4.4 Combined Developmental/Operational Testing

Combined DT/OT is a test event in which DT and OT testers share test assets and data, and in which the events meet both DT and OT requirements. The majority of T&E activities and events in the NECC program will feature combined DT/OT.

3.3.4.5 Information Assurance Testing

IA testing in support of OT will be determined by policy as outline by OSD on 21 Nov 2006 "Policy for Operational Test and Evaluation of Information Assurance in Acquisition Program." IA testing will be addressed through COI #2, Information Management (IM); "Does NECC provide the users with assured information management?" The IA related COI and associated metrics will be assessed based on the six-step process outline in the DOT&E IA policy. An IA Red Team from either a Component or a Service's Information Warfare Centers shall assess Mission Assurance Category (MAC) I and MAC II CMs or groups of CMs assigned a

Confidentiality Level (CL) of Classified or Sensitive and CMs for which the Lead OTA, JST, or DOT&E have specific concern.

TERA for the review of OT Red Team testing at the CM level will use FDCE developmental and development piloting Blue Team results, automated tools (automated port scanners, network packet sniffers, password crackers, and patch management scanners) the DIACAP Scorecard and a DIACAP plan of action and Milestone to determine vulnerability. CMs with unknown, unmitigated medium, or high risk will implement Red Teaming to further define possible vulnerabilities and to develop Tactics, eTechniques, and Procedures (TTPs for mitigation or correction.

Severity and Impact codes will be assigned to failed IA controls to determine risk level associated with the security weakness, the urgency with which corrective actions must take place, and CA assessment of system-wide IA consequences. The CA will establish an Agent of Certification Authority (ACA) to assess Severity and Impact codes. The CA will have an appointed ACA, completed DIACAP Scorecard and System Integration plan prior to the release of an Interim Approval to Test (IATT).

Continuity of Operations (COOP) will be exercised during OT&E for CMs or groups of CMs with an Identified MAC level of I and CMs for which the lead OTA, JST or DOT&E have specific concern. IT System Contingency Plans will be further tested annually with functional tests of major Software revisions.

The JST with DOT&E concurrence will use the results of IA DT&E data during the OTRR in judging whether a CM/s or Increment is ready to enter OT&E. IATT is required as an OT&E entrance criterion.

3.3.4.6 Interoperability Testing

DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," states that "IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS." Joint interoperability certification testing will follow the processes established in the CJCSI 6212.01 series and the CJCSI 3170 series. These processes use an integrated and net-centric approach which dovetails with the CPAS of the NECC program.

Joint Interoperability will be determined through an assessment of compliance with the NR-KPP. NR-KPP evaluations and resulting assessments will be conducted by the JITC) for each NECC CM that introduces joint external interfaces. The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following four elements:

1. Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM)

2. Compliance with applicable GIG Key Interface Profiles (KIP), when mandated
3. Verification of compliance with DoD IA requirements
4. Supporting integrated architecture products required to assess information exchange and use for a given capability

A CDP TEMP annex will provide specific details of the NR-KPP evaluation, assessment, and certification process for NECC.

Interoperability can only be certified against JS J-6 certified requirements, which occurs at the NECC increment level. NR-KPP assessment of each CM will be performed within the context of OMT(s) as the CMs progress through the FDCE, and will be addressed in the respective CM's CMAR. JITC, working closely with the DT and OT Leads for each CM, will leverage findings in their respective tests and provide an assessment of that CM's ability to meet its associated NR-KPP requirements. NR-KPP assessment results will be developed in conjunction with the Capability Provisioning Event Reports (CPERs) and/or CMAR and will be provided to the MDA to support that CM's limited fielding decision.

The NR-KPP assessments provide input to the JITC NR-KPP Certification letter that will be developed in conjunction with the SER. A full or limited interoperability certification will be issued at the NECC increment level, depending on whether all critical interoperability requirements are met and whether there are any discrepancies with critical operational impact. All JITC interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire three years from date of issue.

3.3.4.7 Operational Test

Operational testing of NECC will be conducted continuously at the individual CM level to support CM fielding decisions throughout the development of Increment 1, and with a dedicated IOT&E to resolve overall operational effectiveness and suitability at the increment level. An integrated testing approach will be used to streamline the overall T&E process that embraces the "Test Once" concept. This approach enables OT to use the shared data from CPAS events to provide data/test information to support assessment of MOEs and MOSs to support fielding decisions. The ultimate goal is to have collected sufficient data/test information in the appropriate operational environment throughout the testing process such that by the end of the Operational Piloting event an independent OT assessment of the test data will be sufficient to support the MDA limited fielding decision.

JST, using the RALOT risk assessment process, will determine the level and scope of any OT. The results of OT will be captured in either a CMAR at the CM level, SA at the CDP level, or a SER at the increment level and briefed to the designated decision authority for a fielding decision as discussed in paragraph 3.5. IOT&E is required as the final phase of independent operational testing at the increment level. During this phase of testing, the lead OTA will use previous CMAR and SER reports to assess whether COIs at the increment level have been satisfactorily resolved. This assessment of previous OT reports will determine the overall length and scope of the final phase of IOT&E. IOT&E planning will be documented by the CM TT OT Lead and approved by DOT&E.

3.3.4.7.1 Initial Operational Test and Evaluation

Towards the end of Increment 1 a final phase of IOT&E will be required to address the increment’s overall Operational Effectiveness, Operational Suitability, and Operational Survivability. The scope and focus of the overall IOT&E effort will consider the CM tests and results captured within the assessment reports from throughout the increment. The Milestone C Capstone TEMP will identify the MOEs/MOSs that will be assessed during this phase of test that will be later used to resolve the increment level Critical Operational Issues. The results of IOT&E will be detailed in the increment level SER and will be used to support the MDAs decision to move to Full Operational Capability (FOC) and full fielding at the Full Development Decision Review (FDDR). The Milestone C update to the Capstone TEMP will further define the anticipated scope of the IOT&E with execution details provided in the Operational Detailed Test Plan approved by DOT&E.

3.3.4.8 Reporting Requirements

Table 4 illustrates the test reporting process that will be used for the NECC program that will report the results of DT and OT testing.

Table 4: NECC Program Report Summary

REPORT SUMMARY			
Level	PLAN	REPORT	DECISION/MILESTONE
Increment	TEMP	SER	FDDR
		SER (to support MS C)	MS C
CDP	TEMP Annexes	System Assessment	N/A
CM	O-DTP (Operational Test)	CMAR – supports FDR for CMs	FDR –CMs in context of the mission threads
	D-DTP (Developmental Test)	Capability Provisioning Event Report (CPER)	N/A

This NECC program reporting process will report the results of DT and OT testing as follows:

- **Capability Provisioning Event Reports.** The CPER is a common Joint NECC reporting format that replaces the traditional service DT report. A CPER will detail the findings during all phases of DT. The CPMOs will be responsible for drafting and submitting these reports that will be used to support subsequent DTTR and OTRR.
- **Capability Module Assessment Report.** A CMAR is a test report that is produced for each CM or set of CMs that satisfy a stated mission need. The CMAR aggregates findings of CM testing from the development stage through the operational piloting stage and provides an assessment of CMs ability to satisfy requirements at the CDP level. A CMAR assesses a CM (or multiple CMs) in the context of mission threads and will report on the detailed findings during each phase of OT. These findings will include:
 - CM Limitations,

- MOE, MOS results
- Operational considerations

A CMAR can address one or multiple CMs and will report on the ability of the CM to satisfy a particular mission thread. The CMAR will not provide an effectiveness or suitability recommendation but rather will assess CM MOEs/MOSs which will support resolution of COIs at the CDP level. The CMAR will also support the CM fielding decision at Fielding Decision Review (FDR) as stated in paragraph 3.5.

- **System Assessment (SA).** The SA is a report that supports resolution of COIs identified at the CDP level. This report on the CDP capabilities is based on an aggregation of operational test data/analysis conducted on CMs and reported in CMARs. The combination of SAs and their aggregation of COI resolution at the CDP level will be a primary tool for the OTAs to properly scope the planning and execution of the IOT&E at the increment level.
- **System Evaluation Report.** A SER will serve as a high level OT report that will satisfy the following requirements:
 - **Milestone SER.** For Increment 1, a SER will be provided prior to the Milestone that identifies risk.
 - **Milestone C SER.** During this phase, Milestone C SER will be provided prior to Increment 1 Milestone C and will report on the evaluation of CMs to date. This SER will be used to support a Milestone C decision.
 - **End of Increment SER.** The FDDR is supported by an end of increment SER to resolve COIs that will be tested during IOT&E for Increment 1. This SER will provide an evaluation to assess operational effectiveness and suitability.

3.3.4.9 Deficiency Report Tracking and Correction

The OT&E community will leverage upon the existing NECC Deficiency Reporting process to document CM and FDCE problems and deficiencies or failure to achieve contractual technical performance requirements for both software and hardware. During OT NECC CM anomaly and deficiency reports will be submitted IAW ATEC policy.

3.4 Test Related Documentation Approval Chain Considerations

If the NECC program is to achieve a lean and agile framework that supports rapid fielding, it is vital that representatives of the major stakeholders are empowered to make decisions for their respective commands and that approval of key testing documents are delegated at the lowest level within the organizations as possible.

3.5 Fielding Phase

NECC CMs are fielded upon approval by the MDA or the MDAs designated representative. The NECC program will continually field CMs. There is a single capstone MS C decision for NECC Increment 1, which grants authority for *limited fielding* to operational users and to support OT. Not all Increment 1 CMs are reviewed at Milestone C; rather, the program uses a subset of CMs which is planned to be Global UDOP, Red Track Data, Weather Data, and Blue Force Ground Data CMs associated with CDP #1, SSA. Maturity of this subset of CMs demonstrates

confidence that the FDCE engineering, development, test, and certification processes all work effectively and can be repeated for all CMs throughout the increment to produce militarily useful capabilities for the Warfighter. As subsequent CMs progress through the FDCE process, the JPEO authorizes limited deployment of these CMs to support OT. The decision to then conduct OT on these CMs occurs at OTRRs, which are supported by findings from the lead OTA that the CM has been certified ready to test. This approach differs from a traditional large system development that waits until all required components of the system are ready before fielding can occur. The fielding phase is the final stage of the T&E process and is detailed in Figure 9. Prior to any phase of testing a RALOT will be performed to determine the level of OT in the order as follows:

- **Level I and II Testing.** Upon completion of Level I and II testing, a CMAR will be produced by the lead OTA to report on the CM, or CMs, performance during test. This CMAR will be one of the key documents used by the Decision Authority during FDR to base their limited fielding decision upon.
- **Level III and IV Testing.** For level III and IV, the testing process is modified to allow for an additional phase of OT. Prior to OT, a CPE Report will be used to support an OTRR decision to proceed to OT. Once the CM(s) are certified for Operational Test, OT testing will commence and the lead OTA will produce a CMAR detailing the results of OT. This CMAR will again be one of the key documents used by the Decision Authority during FDR to support their limited fielding decision.
- **IOT&E.** Towards the end of increment 1 a final phase of IOT&E will be required to report the increment’s overall Operational Effectiveness and Suitability and will be captured in the End of Increment SER. During the IOT&E phase the lead OTA will use previous CMAR and Milestone SER reports to determine scope and breadth of the increment level to IOT&E. This SER will be used during FDDR for the designated decision authority to base their decision to move on to FOC for Increment 1.

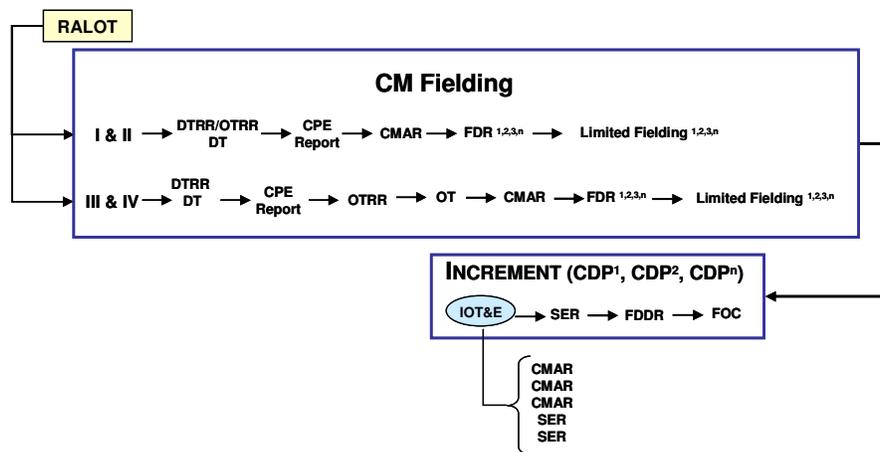


Figure 9: CM/Increment 1 Fielding Process

3.6 Critical Operational Issues

The objective of OT for Increment 1 is to determine the operational effectiveness and operational suitability of NECC. Successful accomplishment of OT will support FDRs following Milestone C at the CM level and an FDDR at the end of Increment 1. Throughout the NECC program COIs will be Jointly developed by the JCCD and the lead OTAs. The critical operational issues for resolution are:

- **COI 1 - Mission Performance (MP):** Does NECC provide C2 information and functional capability necessary to accomplish JC2 critical missions?
 - Scope: Increment 1 will provide capability in the following four MCPs: Intelligence, Force Projection, Force Readiness, and Situational Awareness. The MCPs are referenced and further defined within the CDD. The Mission Capability Packages (MCPs) are then further defined through CDPs. The four MCPs are required to satisfy Mission Performance for NECC Increment 1.
- **COI 2 - Information Management:** Does NECC provide the users with assured information management?
 - Scope: The COI is focused on the ability of NECC to meet the NR-KPP requirements and satisfy Information Exchange Requirements (IER). Therefore, Information Management includes IA and survivability or protection of the capability. The COI is applied to all capabilities developed to support NECC Increment 1. The IERs must meet or improve current mission performance standards.
- **COI 3 - Suitability:** Does NECC provide sufficient availability and usability to give the Warfighter confidence in completing a mission?
 - Scope: The COI looks at the ability of NECC to support mission accomplishment. The focus is in the areas of RAM; Supportability; and Manpower and Personnel Integration (MANPRINT). The systems must be available to the users to provide confidence that a mission can be completed without significant loss of capability. The ability to maintain an operational capability is imperative to Joint C2 missions. Usability, safety and training are key components contributing to NECC's effectiveness.

3.7 T&E Events/Scope of Testing/Scenarios

Future DT and OT events will be captured in respective TEMP Annexes. Below is the formatting example of what DT/OT events/scope of testing/scenarios that should be included in each TEMP Annex.

DT Events:

- **Events.** DT events will be conducted during FY08, 09, and 10 in operationally representative environments with the use of combined DT/OT to the maximum extent possible.
- **Scope of Testing.** DT will examine all performance and technical parameters assigned in the TEC Criteria prior to entering the operational piloting stage of the FDCE. All aspects of operational effectiveness and operational suitability will be evaluated in respective operationally representative environments and the CM will be certified ready for OT. Actual

data, representative of typical NECC data throughput, will be collected and analyzed using FDCE and other distributed facilities.

- **Scenarios.** The scenarios will emphasize the operational realism and will allow for testing to be conducted under various testing environment conditions. The scenarios will be designed to test the operational requirements of NECC and to include representative C2 mission support, information management, detachment support, airborne platforms, afloat and ashore environments, and normal maintenance.
- **Limitations.** The following limitation may impact the conduct of the DT&E.
 - The ability to conduct valid DTs will depend on having sufficient Warfighter participation to exercise and interact with the C2 services provided by NECC. This limitation can be mitigated by engaging JCCD communities early in the planning process to ensure their timely availability.
 - Additional Limitations may be addressed in follow on TEMP Annexes as appropriate.

OT&E Events:

- **Events.** OT events will be conducted during FY08, 09 and 10 in operationally representative environments and will be captured in the respective TEMP Annexes that will outline all planned and approved operational test events.
- **Scope of Testing.** To the greatest extent possible all aspects of operational effectiveness and operational suitability, including information assurance, will be evaluated using the FDCE, which can be linked to operational nodes operating on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). Actual data, representative of typical NECC data throughput, will be collected and analyzed using FDCE and other distributed facilities.
- **Scenarios.** The scenarios will emphasize the operational realism and will allow for testing to be conducted under various environmental conditions. The scenarios will be designed to test the operational requirements of NECC and to include representative C2 mission support, information management, detachment support, afloat and ashore environments, and normal maintenance.
- **Limitations.** The following limitation may impact the conduct of the OT&E.
 - The ability to conduct valid OT&Es will depend on having sufficient Warfighter participation to exercise and interact with the C2 services provided by NECC. This limitation can be mitigated by engaging the user communities early in the planning process to ensure their timely availability.
 - Additional Limitations may be addressed in follow on TEMP Annexes as appropriate.

3.8 Modeling and Simulation

NECC plans to develop and refine architecture products and models in support of M&S strategy for the program. NECC will assess each approved CM packages to determine the amount of the M&S required. Also, NECC will refine and develop additional architecture products and acquire M&S tool to support the level of M&S testing for the program. M&S models will be developed based on Capability Provision Events. Finally, the NECC program plans to refine or develop

additional M&S models based on discussion with the GCCS FoS. Additional M&S test plans will be incorporate in future TEMP annex to illustrate the level of M&S testing and expected outcomes.

M&S, by itself, cannot be used to resolve COIs. The NECC program brings a new paradigm to the DoD in two ways. First, the Business Process Management area deals with how capabilities are provided to the Warfighters. The emphasis in NECC is on quicker fielding of capability in mature CMs. The second aspect is the architecture approach. The plan follows the commercial industry migration toward providing "services" rather than "systems". This is the transformation to a SOA approach. Thus, the application of M&S must address, where appropriate, both Business Process Management and transitioning to a SOA. The NECC M&S Working Group is exploring M&S strategies of several government programs that may have SOAs integral to their architecture. These include Future Combat Systems (FCS), NCES, GCSS, Joint Task Force – Global Network Operations (JTF-GNO), and Network Warfare Simulation (NETWARS). NECC works closely with NCES to benefit from any of their new and evolving M&S tools, services, and capabilities. NECC will not model the network or NETOPS, but will rely on NETWARS to evolve their capabilities to include the SOA services of NCES and NECC. NECC will work with the newly chartered M&S Coordination Office to help broker new DoD and Industry-wide M&S capabilities into NECC. Additionally, NECC expects to capitalize on the newly established DISA Cooperative Research and Development Agreement (CRADA). The NECC program will leverage current Warfighting facilities that specialize in integrating M&S to represent Joint operational environments. USJFCOM's Joint Warfighting Center maintains Joint and Service M&S tools and integrates these capabilities to replicate certified environments for training Joint Task Force Commanders and their staffs.

Existing tools may form the basis of some of the specific M&S requirements identified in the CDD. Thus there are several combat simulators which have been used extensively for early operational assessments of new C2 technology; these include Joint Army Navy Uniform Simulation (JANUS), Joint Theater Level Simulation (JTLS), RESA, and Joint Warfare Simulation (JWARS). As each CDP is being developed, the CPMO will identify those M&S capabilities that currently exist. If they do, they will be SOA-enabled and integrated with other services to meet CDD and VV&A requirements. If they do not exist, then these M&S capabilities will be created along with the supporting services to fulfill the requirements. In terms of planning, the strategy plans to create the specific CDD M&S capabilities integral to the larger intended requirement via work packages to the appropriate CPMO.

4 TEST AND EVALUATION RESOURCES SUMMARY²⁵

4.1 T&E Funding

The NECC JPMO is responsible for providing resources to support Governmental DT&E and OT&E activities. These resources include manpower, funding, materiel, and test equipment. The DT/OT&E activities and resources are outlined in Section 4 of this TEMP at a strategic level. Further details will be detailed in TEMP Annexes, Detailed Test Plans, and specific CM WPs. Updates to the OT resource requirement will be addressed at both the TEMP Annexes and

²⁵ Reference NECC Cost Analysis Requirements Description, 24 April 2007, version 0.2

CDP level. ATEC, as the lead OTA, will collect resource requirements from all the participating OTAs and then coordinate directly with the NECC JPMO T&E Management Branch to ensure adequate OT funding distribution and cost control. Each OTA will track their individual expenditures at the CM level. This effort is required in order to establish an initial baseline of OT funding requirements critical for future NECC T&E planning efforts. The JST will work closely with the JPMO to update this funding baseline as the relationship between CM complexity and OT resource requirements are better understood and captured. Each OTA will use sound business practices and metrics to ensure each CM TT supports this fundamental effort. OTA expenditure reports will be provided at least quarterly, or as requested by the JPMO. The NECC JPMO will provide DT funding directly to each service CPMO as specified in the CM WP to include funding of IA certification/validation activities. OTAs will coordinate activities with each CPMO to ensure maximum efficiency in the conduct of tests and expenditure of resources. The NECC JPMO will fund JITC support of interoperability test certification in accordance with CJCSI 6212.01D. The NECC JPMO and USSTRATCOM funding relationship is addressed in separate correspondence.

4.2 Testing Resources

The testing requirements discussed in this TEMP will detail testing resource requirements at a strategic level. Requirements that are more detailed will be captured in the testing resource section of the respective TEMP Annex.

4.3 Test Articles

The CM, or a collection of CMs, will be the article(s) to be tested. The determining factor is the end-to-end C2 service required by the Warfighter as described in the associated mission threads. Depending on the level of risk projected by Risk Assessments, each individual CM will use the appropriate level of testing resources to mitigate residual risk. Irrespective, each CM (or group of CMs) will be tested to ensure they do not demonstrate a loss of functionality and/or performance of current performance thresholds; and that the CM maintains the desired level of interoperability and complies with the approved security posture.

4.4 Test Sites and Instrumentation

4.4.1 Test Sites

The NECC program leverages upon the current facilities used by the GCCS FoS for test and production. The GCCS FoS facilities are assumed to meet the requirements for the testing and production of NECC capabilities. The equipment and support that will be required to host NECC capabilities and augment existing hardware and software support can be found in the NECC Cost Analysis Requirements Description (CARD) document. Additionally, annexes to this Capstone TEMP (TEMP Annex for Increment 1 CDPs) will include additional test site resource requirements to support DT and OT events when appropriate.

4.4.2 FDCE Lab Facility and JPMO Developmental Hosting Facility

The FDCE is the set of processes and supporting infrastructure that is needed to support the conduct of net-centric CPAS. The FDCE Infrastructure (FDCEI) is the set of distributed hardware and software that is used to implement federated development and certification processes, manage the certification status of CMs, and provide the capability provider community with

web-based screens for managing CPAs. While much of the FDCI is provided by existing Service test and production facilities to include those used for the development of the GCCS FoS, a core FDCE Lab Facility—the FDCE portal—is required. The [FDCE portal](#)²⁶ is currently located within the G2 lab in the DISA Skyline 7 Complex. The FDCE Lab Facility includes an instantiation on both the NIPRNet and the SIPRNet. An additional facility with an internet version of the FDCE is located in a nearby contractor facility and is required for both the development of the FDCE portal and the initial entry into the FDCE for very immature CMs.

Operation and maintenance of the FDCE is conducted by a set of FDCE administrators. These administrators are responsible for operating and maintaining the FDCI, configuring and managing the software and tools used to implement the FDCE process, and providing technical and procedural help to the broader capability provisioning community. It is important to understand that the FDCE will not “host” a CM; rather, a capability provider will host the CM and expose its network access point once the appropriate NETOPS certifications are achieved. This concept holds true for all capability provider communities.

A core set of tools will be made available through the FDCE portal. The JPMO is responsible for the accreditation, licensing, maintenance, funding, SLA, personnel support, and help desk support for these tools. Additional tools will be made available from external Components and agencies. These tools will be hosted and maintained by external organizations. The organization providing the tool is responsible for the accreditation, SLA, personnel support, maintenance and funding, and help desk support for these tools. The JPMO is responsible for obtaining required licenses for DT&E. Determining the types of tools required, based on the needs of each of the Components, is an ongoing JPMO activity. A tool list to support the FDCE is provided within the NECC FDCE portal.

4.4.3 Test and Production Facilities

The following is a summary of the test and production facilities that will be used by the services to support the NECC program.

4.4.3.1 Army Test and Production Facilities

The Army test lab facility located at Ft. Monmouth will perform DT testing as directed by the CPMO and may support other test activities as needed. The hardware needed in the test lab will imitate field configurations. Since there is an initiative for a server consolidation across Battle Command, NECC will be installed on servers currently deployed by Tactical Battle Command (TBC). The servers are the Battle Command Common Server Long Stacks (BCCS-LS) and the Battle Command Common Server Short Stacks (BCCS-SS). The equipment and support that will be required to host NECC capabilities and augment existing hardware and software support at the facility can be found in Appendix M of the NECC CARD.

4.4.3.2 Navy Test and Production Facilities

The SPAWAR Systems Center – San Diego (SSC-SD) laboratories are the Navy’s primary FDCE node. Navy-developed CMs will be hosted at SSC-SD for integration and participation in NECC CPEs during the development and developmental piloting stages. SSC-SD labs provide

²⁶ 25 May 2007, URL: <https://gesportal.DOD.mil/sites/necc/ILS/FDCEOps/default.aspx>

the necessary connectivity to secure and non-secure networks, as well as to Navy data sources such as Link 11, Link 16, Advanced Combat Direction System (ACDS), Officer in Tactical Command Information Exchange Subsystem (OTCIXS), Tactical Data/Digital Exchange System/Subsystem (TADIXS), and Tactical Data Dissemination System (TDDS). Access to data sources not physically co-located with the Navy FDCE node, such as the NITES II weather data server located at North Island Naval Air Station, will be via the network.

The equipment and personnel requirements for the Navy's FDCE node during NECC Increment 1 are identified in Appendix M of the CARD. The Navy FDCE node includes the lab space and hardware necessary to host the anticipated CMs in support of NECC CPEs. The Navy FDCE node architecture and associated costs assume that Navy CMs will run primarily on the GCCS-M system in Increment 1, with accommodation made for non-COE (Common Operating Environment) hosting as well. The stated requirements for the Increment 1 Navy FDCE node are projected based on SSC-SD experience in hosting NECC CMs for development and piloting during the NECC Technology Development (TD) phase. SSC-SD is hosting or supporting six CMs during the TD phase and conducting an average of one technical and one operational CPE for each. Personnel costs included in the FDCE estimate include only lab hardware and software maintenance and administration. Cost of test engineers is included in the estimates for each CM WP, and in the Navy's Software Support Activity estimates. There are no direct costs to NECC for lab space at the SSC-SD facility, and adequate space has been identified for the required equipment and personnel workspaces.

4.4.3.3 Air Force Test and Production Facilities

For Increment 1, no new government or contractor facility requirements are anticipated to meet NECC requirements. Existing government and contractor facilities will be used.

Air Force plans to leverage the existing facilities utilized by the current GCCS-FoS for hardware support, software support, warehousing, and training. The equipment and support that will be required to host NECC capabilities and augment existing hardware and software support at the facility are found in Appendix M of the CARD.

4.4.3.4 USMC Test and Production Facilities

The USMC presently does not have a need for NECC-unique test and production facilities.

4.4.3.5 DISA Test and Production Facilities

DISA will use a facility within an existing DISA location (e.g., Skyline 7) to serve as the FDCE node to support CPMO developmental and operational piloting of capabilities, as well as to serve as the Tier 2 Helpdesk. This facility will have three hardware and software suites that mirror the operational environments. One suite will support developmental piloting; a second suite will support operational piloting; and a third suite will be operationally representative to support integration/interoperability, operational support, and troubleshooting helpdesk problem reports.

4.4.3.6 Operational Support Facilities

There are no new or modernized facilities required for operational support of NECC. NECC plans to leverage the existing facilities used by the current GCCS FoS for hardware support, software support, warehousing, training, and hosting of Tier 1 CMs (e.g., SSC Charleston).

NECC will also leverage existing facilities (DECCs, NOCs, etc) to host NECC Enterprise GCNs and the JTOCC. It is anticipated that Tier 2 and 3 NECC service providers will leverage existing facilities within their organizations/communities of interest to host NECC CMs. (See Appendix D for an explanation of tiered partnerships.) These locations are described in more detail in the NECC CARD and the NECC Technical Operations Architecture document, copies of which are located on the [NECC portal](#)²⁷.

4.4.3.7 JSIC Support Facilities

JSIC maintains a persistent test environment consisting of about 40 major fielded systems of record including a JTF Headquarters and JTF Component C2 systems lab, a JTF planning/logistics systems lab, and a Coalition systems lab. JSIC test labs are connected to NIPRNet, DREN, SIPRNet, Joint Worldwide Intelligence Communications System (JWICS), North Atlantic Treaty Organization (NATO), and CENTRIXS wide area networks. The JSIC C2 system lab is a core node on the Office of the Under Secretary of Defense for Intelligence’s OUSD(I) Distributed Common Ground System (DCGS) Distributed Development and Test Environment (DDTE). The JSIC labs are available under the constraints of the existing JSIC and USJFCOM project prioritization, for NECC T&E activities particularly as the require Warfighter utility and interoperability assessments with fielded capabilities.

4.5 Funding Resources

Table 5 depicts estimated JST manning and OTA funding levels from FY08 through FY10. Details concerning the number of Service lead CMs, the level of CM test, the number of multiple CM testing, location of data collection, Red Teaming support, and other specifics will be included in the TEMP Annexes.

Table 5: JST Manpower/Funding Estimate

	TYPE	RANK	FY07	FY08	FY09	FY10
ATEC				FTE	FTE	FTE
JST Tri-Chair	Civ/Mil	GS-15/O6	1.0	1.0	1.0	1.0
ATEC Representatives to other Service/Agency led JST	CTR	CTR	1.0	1.0	2.0	2.0
ATEC Representatives to other Service/Agency led JST	CTR	CTR	1.0	1.0	1.0	1.0
ATEC Representatives to other Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
ATEC Representatives to other Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
AFOTEC						
JST Rep	Civ/Mil	YS3/YDO3/03-5	.5	0.5	0.5	0.5
AFOTEC Representatives to other Service/Agency led JST	CTR	CTR	.5	1.0	1.0	1.0

²⁷ 25 May 2007, URL: <https://gesportal.DOD.mil/sites/NECC/default.aspx>

UNCLASSIFIED

	TYPE	RANK	FY07	FY08	FY09	FY10
AFOTEC Representatives to other Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
AFOTEC Representatives to other Service/Agency led JST	CTR	CTR	0.0	0.5	1.0	2.0
COTF						
JST Rep	Civ/Mil	GS-13-15/O3-O5	.5	1.0	1.0	1.0
COTF Representatives to other Service/Agency led JST	CTR	CTR	.5	1.0	1.0	1.0
COTF Representatives to other Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
COTF Representatives to other Service/Agency led JST	CTR	CTR	0.0	0.0	2.0	2.0
MCOTEA						
JST Rep	Civ/Mil	GS-13-15/O3-5	0.5	0.5	0.5	0.5
MC Representatives to other Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
MC Representatives to other Service/Agency led JST	CTR	CTR	0.0	0.0	1.0	1.0
JITC						
JST Rep	Civ/Mil	GS-13-15/O3-O5	1.0	0.5	0.5	0.5
JITC Led JST IOP Rep	Civ	GS-14/O3-O5	1.0	1.0	1.0	1.0
JITC Representatives to other Service/Agency led JST	CTR	CTR	1.0	2.0	2.0	2.0
JITC Representatives to other Service/Agency led JST	CTR	CTR	.5	0.0	2.0	2.0
JITC Representatives to other Service/Agency led JST	CTR	CTR	0.0	0.0	2.0	2.0
JITC Representatives to other Service/Agency led JST	CTR	CTR	0.0	0.0	2.0	2.0
		SUB- TOTAL	9	16	26.5	27.5
DISA FSO						
IA Rep to Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
IA Rep to Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
SSC Charleston						
IA Rep to Service/Agency led JST	CTR	CTR	0.5	1.0	1.0	1.0
IA Rep to Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
IA Rep to Service/Agency led JST	CTR	CTR	0.0	1.0	1.0	1.0
USSTRATCOM-DAA						

UNCLASSIFIED

	TYPE	RANK	FY07	FY08	FY09	FY10
DAA Rep to JST	Civ	GS-15/O6	0.5	0.5	0.5	0.5
AT&L						
Action Officer	Gov/Mil	GS-15/O6	0.0	0.0	0.0	0.0
CTR Support to Action Officer	CTR		0.0	0.0	0.0	0.0
CTR Support to Action Officer	CTR		0.0	0.0	0.0	0.0

Table 6: Total NECC OTA Funding Estimates/FY

	FY07	FY08	FY09	FY10
OTA FUNDING	\$.5 MIL	\$ 6.0 MIL	\$ 10 MIL	\$ 15 MIL

Table 7 is a notional estimate of the composition of a standard CM TT. Funding for the development/developmental piloting resource will be provided in CPMO work packages. Operational piloting funding will be provided by the JPMO to the respective OTA.

Table 7: CM TT Manpower Estimate

CM TT	CIV/MIL/CTR	Grade/Rank	FTE
Development/ Development Testing			
Test Officer (CPMO)	Civ/Mil	GS-14/O3-O5	1.0
Asst. Test Officer	CTR	CTR	1.0
IA SME/Tester	CTR	CTR	1.0
NR-KPP SME/Tester	CTR	CTR	1.0
DT SME/Tester	CTR	CTR	1.0
Operational Testing			
Test Officer (OTA)	Civ/Mil	GS-14/O3-O5	1.0
Asst. Test Officer	CTR	CTR	1.0
IA SME/Tester	CTR	CTR	1.0
NR-KPP SME/Tester	CTR	CTR	.5
DT SME/Tester	CTR	CTR	.5

APPENDIX A – ACRONYMS

ACRONYM	DEFINITION
46TS	46th Test Squadron (USAF)
A&S	Assessment and Support
ACA	Agent of Certification Authority
ACAT	Acquisition Category
ACDS	Advanced Combat Direction System
ADM	Acquisition Decision Memorandum
AF	Air Force
AFOTEC	Air Force Operational Test and Evaluation Center
AI	Additional Issue
AoA	Analysis of Alternatives
ASD(NII)/DoD CIO	Assistant Secretary of Defense (Networks and Information Integration) /Department of Defense Chief Information Officer
ATEC	Army Test and Evaluation Command
ATO	Approval to Operate
AV	All Views
BCCS-LS	Battle Command Common Server Long Stacks
BCCS-SS	Battle Command Common Server Short Stacks
C2	Command and Control
C2CIB	Command and Control Capabilities Integration Board
C3I	Command, Control, Communications, and Intelligence
CA	Certification Authority
CAE	Component Acquisition Executive
CARD	Cost Analysis Requirements Description
CCB	Configuration Control Board
CCDR	Combatant Commander
CDD	Capability Development Document
CDP	Capability Definition Package
CELCMC	Communications-Electronics Life Cycle Management Command
CENTRIXS	Combined Enterprise Regional Information Exchange System
CES	Core Enterprise Services
CIO	Chief Information Officer
CIV	Civilian
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual

UNCLASSIFIED

ACRONYM	DEFINITION
CL	Confidentiality Level
CM	Capability Module
CM TT	Capability Module Test Team
CMAR	Capability Module Assessment Report
COA	Course of Action
COCOM	Combatant Commands
COE	Common Operating Environment
COI	Critical Operational Issues
COI	Critical Operational Issue
COMOTEVFOR	Commander, Operational Test and Evaluation Force
CONOPS	Concept of Operations
COOP	Continuity of Operations
COP	Common Operating Picture
CPAS	Capability Provisioning Activities
CPD	Capability Production Document
CPE	Capability Provisioning Event
CPER	Capability Provisioning Event Report
CPM	Component Program Manager
CPMO	Component Program Management Office
CRADA	Cooperative Research and Development Agreement
CTP	Critical Technical Parameter
CTR	Contractor
DAA	Designated Approval Authority
DASD	Deputy Assistance Secretary of Defense
DAU	Defense Acquisition University
DAWIA	Defense Acquisition Workforce Improvement Act
DCGS	Distributed Common Ground System
DDTE	Distributed Development and Test Environment
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DIL	Disconnected/Intermittent/Limited-bandwidth
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DoD	Department of Defense
DoDAF	DoD Architectural Framework
DoDD	DoD Directive
DoDI	Department of Defense Instruction
DOL	Defense Online

UNCLASSIFIED

ACRONYM	DEFINITION
DOT&E	Director of Operational Test & Evaluation
DOT_LPF and Policy	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities and Policy
DS	Defense Systems
DT	Developmental Test
DT&E	Developmental Test and Evaluation
DTC	Developmental Test Command
DTP	Detailed Test Plan
DTRR	Developmental Test Readiness Review
ECP	Engineering Change Proposals
EMT	Engineering Mission Threads
ESC	Electronics Systems Center
FCS	Future Combat System
FDCE	Federated Development and Certification Environment
FDCI	Federated Development and Certification Infrastructure
FDDR	Full Deployment Decision Review
FDR	Fielding Decision Review
FOC	Full Operational Capability
FoS	Family of Systems
FTP	Functionality Transition Plan
GCCS	Global Command and Control System
GCN	GIG Computing Node
GCSS	Global Combat Support System
GES	GIG Enterprise Service
GIG	Global Information Grid
GNO	Global Network Operations
HFE	Human Factor Engineering
I&TP	Integration and Technology Piloting
IA	Information Assurance
IAD	Information Assurance Directorate
IAM	Information Assurance Manager
IAMD	Integrated Air and Missile Defense
IAO	Information Assurance Officer
IATF	Information Assurance Technical Framework
IATO	Interim Approval to Operate
IATT	Interim Authority to Test
IAW	In Accordance With
ICD	Initial Capabilities Document
IER	Information Exchange Requirements

UNCLASSIFIED

ACRONYM	DEFINITION
IEW	Improved Early Warning
IM	Information Management
IOC	Initial Operating Capability
IO-CTA	Information Operations-Capstone Threat Assessment
IOT&E	Initial Operational Test & Evaluation
ISP	Information Support Plan
ISSE	Information System Security Engineer
IT	Information Technology
IT&E	Integrated Test & Evaluation
JAEC	Joint Assessment and Enabling Capability
JANUS	Joint Army Navy Uniform Simulation
JC2	Joint Command and Control
JCCD	Joint Combat Capability Developer
JCD	Joint Capability Developer
JCIDS	Joint Capability Integration Development System
JFC	Joint Force Commanders
JITC	Joint Interoperability Test Command
JKDDC	Joint Knowledge Development and Distribution Capability
JMETC	Joint Mission Environment Test Capability
JMUA	Joint Military Utility Assessment
JNTC	Joint National Training Capability
JPEC	Joint Planning and Execution Community
JPEO	Joint Program Executive Office
JPM	Joint Program Manager
JPMO	Joint Program Management Office
JROC	Joint Requirements Oversight Council
JROCM	Joint Requirements Oversight Council Memorandum
JS	Joint Staff
JS/C/S/A	Joint Staff/COCOM/Services/Agencies
JSIC	Joint Systems Integration Command
JST	Joint System Team
JTC	Joint Training Center
JTF	Joint Task Force
JTF-GNO	Joint Task Force - Global Network Operations
JTLS	Joint Theater Level Simulation
JTOCC	Joint Technical Operations Control Capability
JWAR	Joint Warfare Simulation
JWICS	Joint Worldwide Intelligence Communications System
KIP	Key Interface Profile

UNCLASSIFIED

ACRONYM	DEFINITION
KPP	Key Performance Parameters
KSA	Key System Attributes
M&S	Modeling and Simulation
MAC	Mission Assurance Category
MANPRINT	Manpower & Personnel Integration
MARCORSYSCOM	Marine Corps Systems Command
MCCDC	Marine Corps Combat Development Command
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCP	Mission Capability Package
MCSC	Marine Corps Systems Command
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MIL	Military
MILSATCOM	Military Satellite Communication
MIL-STD	Military Standard
MIW	Mine Warfare
MNS	Mission Needs Statement
MOA	Memorandum of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
MP	Mission Performance
MPA	Maritime Patrol Aircraft
MS	Milestone
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NCES	Net-Centric Enterprise Services
NCOW-RM	Net-Centric Operations and Warfare Reference Model
NECC	Net-Enabled Command Capability
NESI	Net-Centric Enterprise Solution For Interoperability
NETOPS	Network Operations
NETWARCOM	Naval Network Warfare Command
NETWARS	Network Warfare Simulation
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organization
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NITES	Navy Integrated Tactical Environmental System
NMCS	National Military Command System
NOC	NECC Operational Center

UNCLASSIFIED

ACRONYM	DEFINITION
NR-KPP	Net Ready-Key Performance Parameter
NRT	Near Real-Time
NSA	National Security Agency
NSS	National Security Systems
OA	Operational Assessments
OCE	Operational Concept Event
O-DTP	Operational Detailed Test Plan
OMT	Operational Mission Thread
ONI	Office of Naval Intelligence
OPLAN	Operations Plan
OPORD	Operations Order
OPS	Operations
OPTEVFOR	Operational Test and Evaluation Force
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT	Operational Testing
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTC	Operational Test Command
OTCIXS	Officer In Tactical Command Information Exchange Subsystem
OTRR	Operational Test Readiness Review
OUSD (AT&L)	Office of Under Secretary of Defense (Acquisition Technology and Logistics)
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OV	Operational View
PMO	Program Management Offices
PSA	Principal Staff Assistant
PTTA	Provisional Technical Transition Architecture
QC	Quality Control
QOS	Quality of Service
RALOT	Risk Assessment/Level of Test
RAM	Reliability, Availability, Maintainability
RM	Reference Model
RMP	Risk Management Plan
S&S	Space and Spectrum
SA	Situational Awareness
SAML	Security Assertion Markup Language
SATCOM	Satellite Communications
SDD	Systems Development and Demonstration

UNCLASSIFIED

ACRONYM	DEFINITION
SDK	Software Developer Kits
SE	Systems Engineering
SEP	Systems Engineering Plan
SER	System Evaluation Report
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreements
SME	Subject Matter Experts
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SPAWAR	Space and Naval Warfare Command
SPI	Strategic Planning and Information (DISA)
SPS	System Performance Specification
SSA	Software Support Activity
SSC	SPAWAR Systems Center
SSC-SD	SPAWAR Systems Center – San Diego
STAR	System Threat Assessment Report
STD	Standard
SV	System View
T&E	Test and Evaluation
T2	Training Transformation
TADIXS	Tactical Data/Digital Information Exchange System/Subsystem
TBC	Tactical Battle Command
TD	Technology Development
TDDS	Tactical Data Dissemination System
TDS	Technical Data Sheet
TEC	Test, Evaluation and Certification
TECC	Test, Evaluation and Certification Criteria
TEMP	Test and Evaluation Master Plan
TERA	Test and Evaluation Risk Assessments
TOR	Terms of Reference
TPFDD	Time-Phased Force and Deployment Data
TRADOC	Training and Doctrine Command
TRMC	Test Resource Management Center
TRR	Technical Readiness Reviews
TTA	Technical Transition Architecture
TTP	Tactics Techniques Procedures
TV	Technical View
UDOP	User Defined Operational Picture
UFP	User Free Play

UNCLASSIFIED

ACRONYM	DEFINITION
UIC	Unit Identification Code
URL	Uniform Resource Locators
USAF	United States Air Force
USJFCOM	United States Joint Forces Command
USL	Upper Specification Limit
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
USW	Undersea Warfare
V&V	Verification and Validation
VV&A	Verification, Validation, and Accreditation (or Authentication)
VV&A	Verification, Validation, and Accreditation
WIPT	Working-level Integrated Product Team
WP	Work Package
WS	Web Standard
XML	eXtensible Markup Language

APPENDIX B: GLOSSARY OF TERMS

CDP	Product of the Joint Combat Capability Developer (JCCD) process that provides the materiel developer the operational requirements and the functional, behavioral, and performance detail necessary to build a field-ready C2 capability. The CDP contains a description of the desired capability, the conditions under which it must operate, KPP it must meet, and the DoDAF operational views to supplement that information. CDPs convey requirements and operational context necessary to translate Warfighter requirements/capabilities into acquisition/engineering initiatives. A NECC Increment will be comprised of numerous CDPs where each CDP will be comprised of numerous CMs.
Certification	NECC quality control process for ensuring that a maturing CM meets minimum standards of performance, operational utility, net-readiness, and security. Certification occurs when a certification authority (governance body) assesses that a CM has met the entrance criteria established for a CPAS maturity stage.
Certification Decision	A decision to promote a Capability Module from one FDCE stage to the next. Certification does address a CM exiting the FDCE process.
CM	A set of hardware and software components that collectively provide a set of logically grouped, operationally relevant services. Within NECC, all capabilities will be realized and provided through a set of integrated CMs. Aside from capabilities, CMs are expected to provide a logical access point for every security enclave that they support, thus allowing users to access CMs from within the secure environment in which they are already operating.
CMAR	After Milestone C, a Fielding Decision Review (FDR) for CMs is supported by a Capability Module Assessment Report (CMAR). A CMAR can address one or multiple CMs and reports on the ability of the CM to satisfy a particular mission thread. The CMAR is a report on the CM in the context of the mission thread. The CMAR does not provide an operational effectiveness, suitability or survivability recommendation but rather assesses whether the tested CM fulfills requirements and is on track to support overall operational goals. An End of Increment Report or a System Evaluation Report (see definition of SER below) is developed to support the Full Deployment Decision Review (FDDR), and serves to resolve Critical Operational Issues (COIs) for the increment. This report provides an evaluation to assess operational effectiveness, suitability and survivability.
COI	Critical operational issues are those key decision-maker operational concerns that must be answered for the full deployment decision review. They are operationally oriented and not technology, cost, or politically focused. Note that a system is considered operationally ready (effective,

UNCLASSIFIED

suitable, and survivable) to proceed to full deployment when the following operational concerns are answered affirmatively:

- (1) Does the system satisfy the reasons for the operational requirement being established and an acquisition program initiated?
- (2) Can the system accomplish its critical mission(s)?
- (3) Can the system maintain trained preparedness in peacetime for critical mission(s)?
- (4) Can the system be deployed when and where needed for critical missions?
- (5) Can the system be sustained during combat and/or other critical operations?

Note: This does not mean that there are always four or five COIs. These concerns may be adequately addressed in one, three, or more COI as appropriate. However, COIs by their nature are few in number.

CPAS

Net-centric processes for maturing NECC-developed capabilities from initial conception to a state where they are ready to support military operations on the GIG.

FDR

At the culmination of T&E and C&A activities, the MDA conducts an FDR to approve CMs to enter operational use. With a successful FDR decision, a CM transitions from the SDD phase of Increment 1 to the Operations and Support Phase.

Following a favorable OT action and positive CMAR, NECC return to the MDA for the first Fielding Decision Review (FDR). The iterative nature of maturing small packets of capabilities results in multiple FDRs throughout each planned increment. As these may come in quick succession, the MDA may delegate review authority for subsequent FDRs throughout the increment. At successful FDR decisions, the CMs receiving a favorable FDR decision then enter the increment's Operations and Support phase, which overlaps the SDD phase.

FDDR

At the end of SDD, NECC presents the MDA validation that the increment has met its CDD requirements at the Full Deployment Decision Review (FDDR) culminating in Full Operational Capability (FOC) for the increment. The FDDR is supported by an overarching System Evaluation Report (SER) which evaluates operational effectiveness, suitability and survivability.

Decision Reviews – NECC's Increment 1 Milestone B decision initiates NECC as a program of record and an Acquisition Category 1D Major Defense Acquisition Program (MDAP), with Milestone Decision Authority (MDA) delegated to ASD(/NII). There is a single Milestone C for NECC Increment 1, and not all CMs are reviewed at Milestone C. Rather, the program uses a subset of CMs to demonstrate process maturity for Milestone C by validating that the FDCE engineering, development, test, and certification processes all work effectively to produce militarily useful CMs for the Warfighter. A CM's (or group of CMs') operational test activity precedes its FDR. The MDA conducts the first FDR to

authorize software release of the initial subset of CMs to the GIG. The MDA is likely to delegate review authority of subsequent FDRs, which occur throughout the SDD phase as CMs mature. At successful FDR decisions, the CM(s) under review enter the increment's Operations and Support phase, which overlaps the SDD phase. The FDDR serves as the culminating event which closes out the SDD phase for Increment 1.

GIG	The Global Information Grid (GIG) is the organizing and transforming construct for managing information technology (IT) throughout the Department. GIG policy, governance procedures, and supporting architectures are the basis for developing and evolving IT capabilities, IT capital planning and funding strategies, and management of legacy (existing) IT services and systems in the DoD. In discussing the GIG and how a particular program interacts with, supports, or relies upon the GIG, it is useful to think of the GIG from three perspectives-its vision, its implementation, and its architecture. (Source: Defense Acquisition Guidebook, Version 1.6, dtd 24 July 2006)
GIG Architecture	The GIG Architecture is the Department's <i>IT architecture</i> . It describes the implementation component of the GIG, with integrated operational, systems, and technical views. The GIG Architecture fulfills, in part, the requirement to develop a Department-wide enterprise architecture. As defined by the Office of Management and Budget, <i>enterprise architecture</i> is the explicit description and documentation of the current and desired relationships among business and management processes and IT. The Enterprise Architecture describes the "current architecture" and "target architecture," and provides a strategy that will enable an agency to transition from its current state to its target environment. All DoD architectures, including Warfighter, intelligence, business process, and enterprise management architectures, are part of the GIG Architecture. Versions 1 and 2 of the GIG Architecture are the current and target DoD IT architectures, respectively and describe the enterprise view of the GIG.
GIG Implementation Component	The implementation component of the GIG is the existing, globally interconnected, end-to-end set of capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information. The GIG includes all Information Technology (IT) and National Security Systems (NSS) throughout the DoD, and their interfaces to allied and coalition forces, industry, and other Federal agencies. All DoD information systems that currently exist or that have been approved for implementation comprise the GIG. Every DoD acquisition program having an IT component is a participant in the GIG. Each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG. Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, and program managers should consider the existing and planned capabilities of the GIG that might be relevant as they develop their integrated architectures, Joint Capabilities Integration and Development System documentation (see CJCSI 3170.1), and related

	program requirements.
GIG Vision	The GIG vision is to empower users through easy access to information anytime and anyplace, under any conditions, with attendant security. Program managers and Sponsors/Domain Owners should use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. The goal is to increase the net-centricity of Warfighter, business, intelligence, DoD enterprise management, and enterprise information environment management operations by enabling increased reach among the GIG users, increased richness in the information and expertise that can be applied to supporting operational decisions, increased agility in rapidly adapting information and information technology to meet changing operational needs, and increased assurance that the right information and resources to do the task will be there when and where it is required.
MAC I	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures. Mission assurance category (MAC) I systems require high integrity and high availability,
MAC II	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance. MAC II systems require high integrity and medium availability.
MAC III	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. MAC III systems require basic integrity and availability.
MOE	Measure designed to correspond to accomplishment of mission objectives and achievement of desired results (CJCSI 3170.01E). MOEs may be

UNCLASSIFIED

further decomposed into MOPs and MOS.

MOP	Measure of a system's performance expressed as speed, payload, range, time on station, frequency, or other distinctly quantifiable performance features. Several MOPs and/or MOS may be related to the achievement of a particular MOE.
MOS	Measure of an item's ability to be supported in its intended operational environment. MOSs typically relates to readiness or operational availability, and hence reliability, maintainability, and the item's support structure. Several MOSs and/or MOPs may be related to the achievement of a particular MOE.
NECC Tier 1 Development Partners	Those development efforts and products produced under direct funding of the NECC PEO and technical direction of the Chief Engineer and Technical Director. The exact nature of these partnerships will evolve as appropriate to reflect programmatic relationship(s) implemented by higher authority.
NECC Tier 2 Development Partners	Those development efforts not directly funded by NECC but which produce software that will be incorporated into the NECC baseline capability that is implemented by CPMOs. Tier 2 partners will follow NECC architecture and development guidance, and may or may not be under direct technical control of the NECC PM.
NECC Tier 3 Developmental Partners	Those 3 rd party efforts/programs/systems that produce and deploy a capability or product/data that is consumed by NECC and against which NECC requirements can be allocated. These partnerships will be characterized primarily by an MOA and Service Level Agreement (SLA) which establishes the necessary functional, technical, and procedural relationships.
Piloting	An activity that makes not yet fully matured capabilities available to interested parties for experimentation, testing, and evaluation.
PTTA	An initial set of NECC technical guidance is called the Provisional Technical Transition Architecture (PTTA). It is provisional because it is expected that the PTTA will evolve based on the experience and results of the TD phase and that the final architecture, the Technical Transition Architecture (TTA), will not be published until the start of the SDD phase. Key objectives of the NECC PTTA are to minimize the integration problems and to maximize interoperability among NECC capability modules. The NECC PTTA will help eliminate risk during the TD phase and promote rapid progress to the NECC TTA.
RALOT	Risk Assessment Level of Test; the application of OT&E principles to determine the testing guidelines (Level of Test) for a system spiral, increment or block. (Level of Test: I – IV rating determining the rigor involved with testing a spiral.) Level of Test is determined according to the mission impact of the system failure with respect to the likelihood of

UNCLASSIFIED

failure within the spiral. [Mission Impact: The impact of a spiral failure within its operational environment. Likelihood of Failure: An assessment of the likelihood of failure from different threats to success.]

SEP

The System Evaluation Plan (SEP) is the primary ATEC planning document for an independent system (CM(s) in the case of NECC) evaluation and assessment so as to ensure that only operationally effective, suitable, and survivable Army and multi-Service capabilities are delivered to the users. Critical to the decision making process is the availability of unbiased, objective evaluations and assessments of a system's capabilities. Capabilities evaluation integrates experimentation, demonstration, and M&S information with available test data to address the evaluation issues (that is, CTPs, COIC and any Additional Issues developed by the system evaluator). Through the SEP, the need for testing is determined and unnecessary testing avoided. The SEP documents the evaluation strategy and overall test/simulation execution strategy of a system for the entire acquisition cycle through fielding. The detailed information contained in the SEP supports concurrent development of the TEMP or TEMP Annex. The SEP is focused on evaluation of the system in the context of mission accomplishment, performance, safety, health hazard, and operational effectiveness, suitability, and survivability. The system evaluator, in coordination with the T&E WIPT / JST, prepares the SEP.

SER

As a set of capabilities approaches a fielding or full deployment decision review, a System Evaluation Report (SER) is produced to advise the decision review principals and milestone decision authority concerning the adequacy of testing, the system's operational effectiveness, suitability, and survivability, as well as recommendations for future T&E and system improvements. For a major defense acquisition program (MDAP), the system evaluation in support of the full deployment decision review will use data resulting from the IOT as a major data source integrated with other credible data sources. The capabilities evaluation focuses on demonstrated technical and operational characteristics, performance, and safety as a part of the capability's operational effectiveness, suitability, and survivability. System assessment examines a system's existing and potential capability so as to identify risks particularly when there is continuing development effort.

SPS

Measurable critical system characteristics that, when achieved, allow the attainment of desired technical performance capabilities within a CM.

APPENDIX C: REFERENCED DOCUMENTS

NECC DOCUMENT	DESCRIPTION	MILESTONE NEEDED	GOVERNMENT POC
Analysis of Alternatives (AoA), IDA, July 2005	Documents critical technologies associated with concepts, including technology maturity, technical risk and technology maturation and demonstration	MS A	NII
Acquisition Program Baseline (APB), TBD	Documents cost, schedule, and KPP objective and threshold values prior to program initiation	MS B and C	NECC Program Control Branch
Acquisition Strategy (AS), TBD	Describes schedule, cost, and funding activities and issues associated with system implementation	MS B and C	NECC Program Control Branch
Architecture Framework Document	Describe the high-level architectural concepts and constructs that are applicable across all three planned increments of NECC	MS B	NECC System Engineering Branch
Capabilities Development Document (CDD), 7 June 07	Documents NECC capabilities, requirements, and performance attributes as part of an evolutionary development strategy	MS B	USJFCOM
Clinger Cohen Act (CCA) Package, 7 March 2006	The CCA Compliance Report documents compliance with the CCA's performance based principles for acquiring and managing information technology	MS A, B and C	NECC Program Control Branch
Component Cost Analysis, TBD	Cost analysis for NECC components	MS B	NECC Program Control Branch
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
Economic Analysis (EA), TBD	Cost and benefit analysis for selecting the most efficient and cost effective development strategy	MS B	NECC Program Control 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

UNCLASSIFIED

NECC DOCUMENT	DESCRIPTION	MILESTONE NEEDED	GOVERNMENT POC
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-Centric Enterprise Services (NCES) Systems Engineering Plan (SEP) V0.95, 20 September 2005	Systems engineering processes and the integration of the process with the management, support, and acquisition processes	MS B	NCES
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
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

DIA-Published Threat Documents

- (U) Transformational Communications Satellite System Threat Assessment Report, NASIC-1574-4388-06, September 2006, (S//NF//MR).
- (U) Future Combat System (FCS) Brigade Combat Team (BCT) System Threat Assessment Report, 7 February 2007, (S//NF).
- (U) Chemical, Biological, and Radiological Warfare Capstone Threat Assessment, DI-1650-83-06, June 2006, S//FGI GBR//NF//MR).
- (U) Information Operations Capstone Threat Assessment, (IO-CTA) 5th Edition (U), DI-1577-33-06, Volumes 1-8, 10-14, and 16, January 2006, (S//NF/202912022).
- (U) Naval Electronics, Navigation, and Networked Systems (NENNS) Capstone System Threat Assessment, ONI-CTA-055-06, September 2006, (S//NF//20310615).
- (U) Space Capstone Threat Assessment, DoD-1574-0727-06, March 2006, (S//FGI//NF//MR).

DISA Documents

- DISA Instruction 610-225, Information Services, DISA Acquisition Oversight and Management, "Managing the Delivery of IT Capabilities: The DISA Strategic Approach," August 2003.
- DISA Net-Centric Enterprise Services: Systems Engineering Process Architecture, draft, March, 2004
- DISA Systems Engineering Process, v2.0, December 16, 2004.

DoD Documents

- ASD(NII)/DoD CIO Net-Centric Checklist v2.1.3, 12 May 2004
- DoD Instruction 8510.1-M, Certification and Accreditation Process (DITSCAP) Application Manual, July 31, 2000.
- CJCSI 3170.01E Joint Capabilities Integration and Development System, May 11, 2005
- CJCSI 6212 Interoperability and Supportability of Information Technology and National Security Systems]
- CJCSM 3170.01B, Operation of the Joint Capabilities Integration and Development System, May 11, 2005
- CJCSI 3170.01C
- CJCSI 6212.01B
- CJCSI 6212.01C
- CJCSI 3151.01
- CJCSM 3170.01
- CJCSM 6715.01A
- DCIO DoD Net
- DCIO Guidance and Policy Memorandum 8
- Defense Test and Evaluation Management Guide

UNCLASSIFIED

- Department of Defense Architecture Framework (DoDAF), Version 1.5, Volume I: Definitions and Guidelines, DoDAF Working Group, 23 April 2007.
- DoD Directive 0-8530.2, “Computer Network Defense”, March 9, 2001.
- DoD Directive 0-8530-1-M, “Computer Network Defense Certification and Accreditation Program”.
- DoD Directive 5000.1, “The Defense Acquisition System,” May 12, 2003.
- DoD Directive 5200.1 “DoD Information Security Program”, December 13, 1996.
- DoD Directive 8001.1
- DoD Directive 8500.1, “Information Assurance (IA)”, October 24, 2002.
- DoD Instruction 5000.2, “Operation of the Defense Acquisition System,” May 12, 2003.
- DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997.
- DoD Manual 8510.1-M, “Department of Defense Information Technology Security.
- DoD Memorandum, “Enterprise Services Roundtable – Early Adopter Program Selection”, November 10, 2003.
- DoD/OSD memo: Implementing Systems Engineering Plans in DoD – Interim Guidance; AT&L, March 30, 2004.
- DoD Instruction 4630, 4680
- DoD/OSD Memo: Policy for Systems Engineering in DoD; AT&L, February 20, 2004
- DoD/OSD Systems Engineering Policy Addendum, October 22, 2004.
- DIACAP (“DoD Information Assurance Certification and Accreditation Process” – DoD Instruction 8510.bb), Supersedes DoDI 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)”.
- OSD AT&L Systems Engineering Plan (SEP) Preparation Guidance, V1.0, August 15, 2005.
- Office of the Secretary of Defense - Operational Test and Evaluation, 16 June 2003, Memorandum for Distribution, *Subject: Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments.*
- Office of the Secretary of Defense Director - Operational Test and Evaluation, 21 November 2006, Memorandum for Distribution, *Subject: Policy for Operational Test and Evaluation of Information Assurance in Acquisition Program.*
- System Engineering Fundamentals, Defense Acquisition University, 2001.
- JROCM 202-02 GIG Mission Area ICD, 22 Nov 2002.
- Joint Program Management Handbook, Defense Acquisition University, Third Edition, July 2004.
- Defense Acquisition Guidebook, Defense Acquisition University, November 2004.
- DoD Defense Acquisition University (DAU) DEFENSE ACQUISITION ACRONYMS AND TERMS, 11th Edition.

Systems Engineering Standards and Best Practices

- ANSI/EIA 632, Processes for Engineering a System, 1998.
- IEEE 1220, Application and Management of the Systems Engineering Process, 1998.

UNCLASSIFIED

- INCOSE Systems Engineering Handbook, version 2a, 1 June 2004.
- ISO/IEC 15288, System Life Cycle Processes, 2002
- SEI Capability Maturity Model Integration (CMMI) for Systems Engineering (SE)/Software Engineering (SW)/Integrated Product and Process Development (IPPD)/Supplier Sourcing (SS), Version 1.1 Continuous Representation, CMU/SEI-2002-TR-011, 2002.
- System Engineering: Principles and Practices; A. Kossiakoff and W.N. Sweet; Wiley; 2003

Air Force

- Global Command and Control System–Air Force Family of Systems (GCCS-AF FoS) Systems Engineering Plan (SEP), Version 1.0, January 10, 2006

Other Referenced Documents

- GIG Capstone Requirement Document
- Global Information Grid (GIG) Enterprise Services Interim Capability Document
- Joint Publication 1-02
- Net-Centric Operations & Warfare Reference Model v0.9, modified 30 June 2003
- Joint Publication 6-02
- Joint Publication 3-13
- JBM C2 Road Map
- NECC Provisional Technical Transition Architecture Specification v0.5.7, dated 12 April 2006
- CDP Developer Guide, JCCD Process Docs

APPENDIX D: TEST, EVALUATION, AND CERTIFICATION CRITERIA

Metrics and evaluation criteria are available at:

<https://gesportal.dod.mil/sites/necc/blank9/default.aspx?RootFolder=%2fsites%2fnecc%2fblank9%2fTesting%20%20Evaluation%20Documents%2fTEC%20Criteria&View=%7bDEC845E4%2d622C%2d466C%2d9CF7%2d6F34406A286B%7d>

APPENDIX E: REFERENCES

Document Referred Links

Note: Access to the links listed below will depend on your user access privilege to them as well as to the storage of this document when saved.

Acquisition Strategy:

https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

Architectural Framework:

https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

Configuration Management Plan:

https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

IA Strategy:

https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

JCCD Management Process:

<https://gesportal.DOD.mil/sites/necc/JCCD/default.aspx?RootFolder=%2fsites%2fnecc%2fJCCD%2fShared%20Documents%2fNECC%20JCCD%20Indoctrination&View=%7b965E7E59%2d36DB%2d4B1A%2dBA56%2d270B330F1224%7d>

NECC CPAS CONOPS:

https://gesportal.dod.mil/sites/necc/doc_status/default.aspx

NECC CPE SOP:

<HTTPS://GESPORTAL.DOD.MIL/SITES/NECC/INTEGRATION/DOCREPOSITORY/DEFAULT.ASPX?ROOTFOLDER=%2FSITES%2FNECC%2FINTEGRATION%2FDOCREPOSITORY%2FSHARED%20DOCUMENTS%2FCPE%20SOP&VIEW=%7B06C52759%2DC601%2D4BEC%2DAA0B%2D44A2ECB54DCB%7D>

NECC UFP SOP:

<https://gesportal.DOD.mil/sites/necc/integration/DocRepository/default.aspx?RootFolder=%2fsites%2fnecc%2fintegration%2fDocRepository%2fShared%20Documents%2fcpe%20sop&View=%7b06C52759%2dC601%2d4BEC%2dAA0B%2d44A2ECB54DCB%7d>

UNCLASSIFIED

APPENDIX F: POINTS OF CONTACT

A list of contacts is available at:

<https://gesportal.dod.mil/sites/necc/TE/TE%20WIPT/default.aspx?RootFolder=%2fsites%2fnecc%2fTE%2fTE%20WIPT%2fShared%20Documents%2fAdministrative%20Information&View=%7b2C2099D3%2d1651%2d455E%2d834B%2d6DCDF16D9191%7d>

UNCLASSIFIED