Net-Enabled Command Capability

LOGISTICS SUPPORT ANALYSIS

(LSA)

12 July 2007

Version 1.0.0

Prepared by:

NECC
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

In Collaboration with the NECC Component Program Managers
for the Navy, Air Force, Army, Marine Corps, JFCOM and DISA

APPROVAL PAGE

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

LAURA D. KNIGHT

Program Manager,
Joint Program Management Office (JPMO),
Net-Enabled Command Capability (NECC)

EXECUTIVE SUMMARY

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD) principal capability for conducting Joint Command and Control (C2). NECC will provide the capability to plan, execute, monitor, and assess collaborate with Joint and multinational operations by enabling vertical/horizontal information exchange across the Joint/coalition C2 community. NECC will facilitate the exchange of information across multiple security domains and reduce logistics/support requirements for system administration, operations, training, and maintenance.

This Logistics Support Analysis (LSA) documents the management approach, decisions, and plans associated with the Integrated Logistics Support (ILS) elements. This document is prepared in compliance with DoD Directive (DoDD) 5000.1, DoD Instruction (DoDI) 5000.2, and the Defense Acquisition Guidebook (DAG)[1]. Careful consideration of logistics resource requirements ensures affordable, effective support strategies that satisfy the goals for operational effectiveness, optimum readiness, and the facilitation of iterative technology enhancements during the system lifecycle.

The ILS challenge for NECC, which is based on Service Oriented Architecture (SOA), is sustainment activities that are not performed by a single organization. Sustainment responsibilities are spread across many materiel providers managed by the applicable Component Program Management Offices (CPMO). These organizations are responsible for core sustainment of Capability Modules (CMs), while the NECC Joint Program Management Office (JPMO) is responsible for sustainment relating to NECC infrastructure activities. Service Level Agreements (SLA) negotiated with the NECC JPMO by materiel providers includes sustainment requirements and metrics.

NECC ILS involvement early in the program with systems engineering, integration and technical piloting, test and evaluation, configuration management, and training provides an integrated approach for effectively supporting NECC C2 capability throughout the lifecycle. Since NECC is both a Major Automated Information Systems (MAIS) and a program with fewer physical manifestations than others of comparable size and scope, whose logistics needs was considered throughout the acquisition process. Logistics requirements need to be incorporated into the Product Support Strategy (PSS), which is progressively refined during succeeding acquisition phases.

Supportability is incorporated into the design and development of NECC to shape and influence the support concept and associated lifecycle costs for the ten core logistics elements.

---

[1] Defense Acquisition Guidebook (DAG), Chapter 5.1.2, 16 Dec 2004, https://akss.dau.mil/dag/DoD5000.asp?view=document

REVISION HISTORY

VERSION NUMBER	REVIEWER/ ORG	CHANGES	VERSION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
0.01.11 Draft	R. Lyle	SAIC QA	1 Jun 07	8 June 07	R. Lyle
0.01.10 Draft	R. Lyle	TDPS Branch	3 May 07	22 May 07	R. Lyle
0.01.9 Draft	R. Lyle	Updated info from Doc Rev Board	5 Apr 07	4 Apr 07	R. Lyle
0.01.8 Draft	R. Lyle	Updated info from CPMOs/ILS WG	16 Mar 07	13 Mar 07	R. Lyle
0.01.7 Draft	R. Lyle	Updated info from CPMOs/ ILS WG	22 Feb 07	25 Feb 07	R. Lyle
0.01.6 Draft	R. Lyle	Updated info from CPMOs/ ILS WG	16 Feb 07	20 Feb 07	R. Lyle
0.01.5 Draft	R. Dean	Updated info from CPMOs/ ILS WG	26 Jan 07	28 Jan 07	R. Dean
0.01.5 Draft	R. Dean	Updated info from CPMOs/ ILS WG	11 Jan 07	15 Jan 07	R. Dean
0.01.4 Draft	R. Dean	Updated info from CPMOs/ ILS WG	5 Dec 06	8 Dec 06	R. Dean
0.01.3 Draft	R. Dean	Updated info from CPMOs/ ILS WG	28 Nov 06	1 Dec 06	R. Dean
0.01.2 Draft	R. Lyle	Updated info from CPMOs/ ILS WG	25 Oct 06	22 Nov 06	R. Lyle
0.01.1 Draft	R. Lyle	Updated info from CPMOs /ILS WG	16 Oct 06	18 Oct 06	R. Lyle
0.1.12	DLB/SPEC	Edited and formatted document for final approval	2 July 2007	2 July 07	Dustan Brown
0.1.0	DLB/SPEC	Final formatting, inserted new title page, revised Approval page, updated hyperlinks, and removed draft watermark	11 July 2007	11 July 07	Dustan Brown

All hyperlinks embedded in this document will require users to register for the Defense Online (DOL) Portal. Please follow this link to complete your registration: Defense Online

TABLE OF CONTENTS

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

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

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

LIST OF FIGURES ..... **VII**

LIST OF TABLES ..... **VII**

1 INTRODUCTION **1**

1.1 BACKGROUND 1
1.2 PURPOSE 1
1.3 SCOPE 1
1.4 RELATIONSHIP TO OTHER NECC DOCUMENTS 2

2 PROGRAM OVERVIEW **2**

3 ANALYSIS SUMMARY **2**

3.1 HOSTING APPROACH 2
3.2 OPERATIONS (OPS) CAPABILITY CONCEPT 2
3.3 NECC CLIENT SELECTION 3

4 OPERATIONS AND SUPPORT SYSTEM **3**

4.1 NECC MISSION 3
4.2 FIELDING/OPERATIONS/SUSTAINMENT 4
4.2.1 Fielding *4*
4.2.2 Operations *4*
4.2.3 Sustainment *4*
4.3 BASING CONCEPT 5
4.4 BASING AND DEPLOYMENT DESCRIPTION 5
4.4.1 Virtualization *6*
4.4.2 GIG Computing Nodes *6*
4.4.3 NECC Virtualization Requirements *7*
4.5 INTERFACES AND SUPPORTING SYSTEMS 8
4.6 OPERATING ENVIRONMENTS 8
4.7 ARCHITECTURE 8
4.8 LEGACY SYSTEMS IMPLEMENTED IN NECC 9
4.9 CURRENT GCCS FOS MAINTENANCE AND OPERATIONAL SUPPORT SYSTEMS 9
4.10 NECC MAINTENANCE AND OPERATIONAL SUPPORT SYSTEMS 9
4.10.1 NECC Joint Technical Operations Control Capability Concept *9*
4.10.2 Roles and Responsibilities *10*
4.10.3 Delivering New or Updated CMs to the Warfighter *11*
4.10.4 NECC Help Desk Tiered Structure *12*
4.10.5 JTOCC *13*
4.10.6 NECC-wide Runtime Governance *13*
4.11 RESOURCES REQUIRED TO SUPPORT EXISTING GCCS FOS SYSTEMS 14
4.12 RESOURCES REQUIRED TO SUPPORT PROPOSED NECC SYSTEMS 14
4.12.1 Net-Centric Enterprise Services *14*

5 INTEGRATED LOGISTICS SUPPORT **15**

5.1 NECC MAINTENANCE PLANNING 15
5.1.1 NECC Hardware *15*
5.1.2 NECC Capability Nodes *16*

5.1.3 NECC Remotely Supported Sites 17
5.1.4 NECC Locally Supported Sites 17
5.1.5 NECC Software 18
5.1.6 FDCE Hardware and Software Support 19
5.2 SUPPLY SUPPORT 19
5.3 SUPPORT AND TEST EQUIPMENT 19
5.4 MANPOWER AND PERSONNEL 19
5.5 TRAINING AND TRAINING SUPPORT 21
5.6 TECHNICAL DATA 21
5.7 COMPUTER RESOURCES 22
5.8 FACILITIES 22
5.9 PACKAGING, HANDLING, STORAGE AND TRANSPORTATION (PHS&T) 22
5.10 DESIGN INTERFACE 23

6 DETERMINATION OF LOGISTIC RESOURCE REQUIREMENTS 23

6.1 SUPPORTABILITY AS AN INTEGRAL PART OF THE SYSTEMS ENGINEERING PROCESS 25
6.2 SUPPORTABILITY ANALYSES PROCESS 25
6.3 SA CONCEPTS THROUGHOUT THE LIFE CYCLE 27
6.4 SUPPORTABILITY ANALYSES REPORTS 27
6.5 NECC SUPPORT CONCEPT 28
6.6 MANAGED SERVICES STRATEGY 28
6.6.1 Administration 28
6.6.2 Storage Solutions 29
6.6.3 Performance Monitoring 29
6.6.4 Secure Server Builds and Intrusion Detection Systems 29
6.6.5 Capacity Management 29
6.6.6 Capability Maturity Model Integrated (CMMI) Level of Attainment or Equivalent 29
6.6.7 Network Availability 29
6.6.8 Connectivity 30
6.6.9 Network Access and Security 30
6.6.10 Scalability 30
6.6.11 Disaster Recovery 30
6.6.12 Facility Description 30

7 TEST AND EVALUATION 31

7.1 TEST AND EVALUATION STRATEGY 31

8 SUPPORTABILITY AND PERFORMANCE REQUIREMENTS 31

8.1 KPPS 31
8.2 MEASURES OF EFFECTIVENESS AND SUITABILITY 31

9 NECC ACQUISITION STRATEGY 32

9.1 ACQUISITION APPROACH 32

10 COST ESTIMATES AND FUNDING 32

11 TECHNOLOGY REFRESH 32

12 BUSINESS PROCESS IMPROVEMENT 32

13 DEMILITARIZATION AND DISPOSAL 32

14 SUPPORTABILITY AND RISK 32

14.1 RISK MANAGEMENT STRATEGY 33

15 CONFIGURATION MANAGEMENT 33

15.1 ENGINEERING REVIEW BOARD (ERB) 33

16 INFORMATION ASSURANCE STRATEGY 33
17 RECOMMENDATIONS 34
APPENDIX A – ACRONYMS 35

LIST OF FIGURES

Figure 1: NECC Increment 1 Physical Architecture 7
Figure 2: CM Deployment and Provisioning Process 11
Figure 3: NECC Site Architecture 16
Figure 4: Remotely Supported Site 17
Figure 5: Locally Supported Site 18
Figure 6: NECC JPMO Organization 21
Figure 7: Supportability Analyses Process 26
Figure 8: How Do You Do Supportability Analyses? 26
Figure 9: Supportability Analyses Reports 27

LIST OF TABLES

Table 1: NECC Locations 6
Table 2: Approximate Operational Manpower Requirements 20

1 INTRODUCTION

1.1 Background

The Net-Enabled Command and Control (NECC) Capability of the Department of Defense is the principal Command and Control (C2) capability accessible in a net-centric environment and focuses on providing commanders and Warfighters with data and information needed to make timely, effective, and informed decisions. NECC draws from the C2 community to provide current and new C2 capabilities into a fully integrated, interoperable, and collaborative Joint solution.

1.2 Purpose

This LSA ensures that supportability is included as a system performance requirement[2] and ensures that the system is developed or acquired with an optimal support system and infrastructure. This Logistics Support Analysis (LSA) was developed in coordination with the Integrated Logistics Support (ILS) Working Group, which is composed of the Joint Program Management Office (JPMO), Component Program Management Offices (CPMOs), and NECC program development branches[3].

1.3 Scope

This LSA determines an optimal set of logistic resource requirements for the system to achieve effectiveness at a minimal life cycle cost, while minimizing the total logistic footprint. This LSA is an integral part of the overall Systems Engineering Supportability Analysis for NECC. It aligns with the objectives of Increment 1, as outlined in the Acquisition Strategy. The LSA provides a baseline for development of the NECC Product Support Strategy (PSS). For information on the PSS, see **Defense Acquisition Guidebook[4], Chapter 2.3.12**.

Supportability is a design characteristic. Early logistics supportability analyses results in the establishment of support-related parameters[5] that specifically relate to systems readiness objectives and support costs. Achieving and sustaining affordable system supportability is a lifecycle management function. Supportability analyses are integral parts of Systems Engineering (SE). A wide range of related analyses needs to be conducted within a sound SE process.

The NECC Net-Ready Key Performance Parameters (NR-KPP) requires interoperability and supportability. As part of the acquisition strategy, the program develops and documents a PSS for lifecycle sustainment and continuous improvement of product affordability, reliability, and supportability, while sustaining readiness. The NECC LSA is the principal logistics input to the NECC PSS.

---

[2] By providing the basis for conducting a Product Support Strategy which does address these requirements.

[3] MIL-HDBK-502 Department of Defense Handbook Acquisition Logistics, dated 30 May 1997

[4] Defense Acquisition Guidebook, Chapter 2.3.12, dated 16 Dec 2004, http://akss.dau.mil/dag/GuideBook/IG_c2.3.12.asp

[5] For example, by performing a Failure Modes Effects and Criticality Analysis (FMECA) or a Failure Modes Effects Analysis (FMEA).

1.4 Relationship to Other NECC Documents

The NECC LSA relates to numerous NECC documents. A crosswalk between other NECC documents and their relevance to the LSA is shown ctrl-click **here**[6].

2 PROGRAM OVERVIEW

The NECC program will be responsive to the Warfighter through tightly coupled capability needs, development, test, and user engagement processes. The program leverages existing and evolving C2 capabilities and centers of excellence with its "A-B-C" commitment to "Adopt-before-Buy, Buy-before-Create." The key to ABC is adaptation of commercial best practices, architectures, and standards for C2. The NECC program ensures that our C2 capability evolves towards increased net-centricity and Joint mission integration.

3 ANALYSIS SUMMARY

3.1 Hosting Approach

Three alternatives (appliance, software-only, and virtualized environment) were considered for the hosting of NECC Capability Modules (CMs). In the appliance alternative, NECC fields and maintains a turnkey integrated hardware-software solution to both enterprise and local computing nodes. For this option, NECC maintains configuration management over the computing environment and can ensure that performance requirements are met. In the software-only alternative, NECC develops software solutions and provides them to the Services to field Service-provided hardware solutions. This approach introduces complexity by requiring materiel providers to develop software solutions capable of running on multiple, unspecified hosting environments. In the virtualized environment alternative, NECC develops software solutions capable of running on Service-provided Global Information Grid (GIG) Computing Nodes (GCNs) that meet a set of minimum requirements (e.g., x86-based processor running VMWare). NECC then provisions CMs into a virtualized environment running on the GCN. The virtualized environment alternative was selected for the following reasons:

1. Amount of Service buy-in
2. Compatibility with ongoing DoD and Service infrastructure initiatives
3. Lower integration risk than software-only alternative

3.2 Operations (Ops) Capability Concept

Three alternatives (centralized, distributed, and hybrid) were considered for the Operations and Maintenance (O&M) of NECC CMs. In the centralized alternative, all O&M functions are performed from a centralized Enterprise Management Center over the wide area network. In the distributed alternative, all O&M functions are performed by the local hosting organization. This alternative is considered to be the most costly. In the hybrid alternative, many O&M functions (e.g., automated software distribution, security patches, and performance monitoring) will be performed from a centralized location, while the local hosting organization will operate and

---

[6] Table 1-1 "NECC Documentation and LSA Relationships", accessed 2 July 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared%20Documents/LSA%20Links/Relationship%20to%20Other%20NECC%20Documents.doc

maintain their Local GNCs up through the virtualized machine monitor. The hybrid approach was chosen due to its close alignment with the virtualized hosting environment approach selected for hosting NECC CMs. Ops Capability Concept Selection Criteria:

1. Type of environment where O&M functions are hosted (centralized or localized)
2. Cost
3. Compatibility with the Hosting Approach

The Ops Capability Concept alternative selected was the hybrid, in which many O&M functions (e.g., automated software distribution, security patches, and performance monitoring) will be performed from a centralized location, while the local hosting organization will operate and maintain their Local GIG Computing Node up through the virtualized machine monitor, as opposed to the Centralized Concept alternative or the Distributed Concept alternative. The selection criteria were (1) the type of environment where O&M functions are hosted, (2) the cost, and (3) the compatibility with the selected Hosting Approach (virtualized environment).

3.3 NECC Client Selection

Two alternatives (thick clients or thin clients) were investigated for the NECC client solution. (1) thick clients do as much processing as possible and only pass data for communications and storage to the server, and (2) thin clients are computers or client software in client-server architecture networks, which depend primarily on the central server for processing activities, and mainly focus on conveying input and output between the user and the remote server. NECC choose a thin-client approach. The program based this decision on the following selection criteria:

1. Amount of software planned to operate with a web-browser environment (more is better)
2. Amount of special-purpose software required (less is better)

NECC software will be predominantly written to run within a web-browser, allowing end-users to use their existing Service-provided computers to access NECC CMs. In some cases, NECC software components will be projected into the client browser (e.g., browser plug-ins). In some cases, in order to meet performance requirements, NECC may require special-purpose software to be installed on end-user computers, but this type of solution is to be avoided when possible. NECC does not plan on fielding special-purpose client-hardware devices.

4 OPERATIONS AND SUPPORT SYSTEM

4.1 NECC Mission

This Capability Development Document (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 National Military Command System (NMCS), Joint Force Commanders (JFC), Service and Functional Component Commanders, and subordinate Service commands. 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.

4.2 Fielding/Operations/Sustainment

4.2.1 Fielding

NECC will continuously field CMs. Refer to NECC Increment 1 Technical Operations Architecture for further information on the NECC fielding. CPMO fielding consists of the activities that directly provide capabilities to the operational Warfighters. These activities include training, logistics provisioning, and deployment of any required hardware and software. As part of its Implementation Strategy, CPMO fielding preparation begins by clearly identifying the operational environment and platform applicability for particular CMs planned for development by NECC. The overriding CPMO principle for fielding is that the final decision to update Service C2 capabilities in a command lies with the Operational Commander. Therefore, while new versions or new capabilities may become available from NECC, major commands decide if and/or when CMs are fielded to their commands.

4.2.2 Operations

NECC operations are based on the net-centric concept of software services accessible via network access, independent of a specific Warfighter platform. The Warfighter accesses NECC CMs using a standard web access device and does not require client platform-specific NECC software. Physical location of the CMs is independent of the user's location. Thus, NECC operations are substantially different from more traditional client-server-oriented C2 systems where most of the mission-application software is co-located with Warfighter.

NECC operations include CM execution monitoring. The monitoring is focused on service availability and compliance with SLAs. NECC technical operations control capability acts as the primary interface to the Joint Task Force – Global Network Operations (JTF–GNO) operations support for issues relating to GIG network access and performance, as well as the Defense Information Systems Agency (DISA) NetOps Centers (DNC) for monitoring and managing network operations.

4.2.3 Sustainment

NECC ensures the provision of sustainable Joint Warfighter capabilities and emphasizes transformational technology and operations. NECC seeks transformational technologies with complementing tactics, techniques, and procedures. Coalitions of partnerships warrant pursuit to the maximum extent possible, with components engaging in joint ventures, seeking equitable new processes to file and sustain joint capabilities.

NECC JPMO led the fielding and the sustainment of CMs. The NECC JPMO Technology Develop Phase Support (TDS) Branch is the lead for sustainment issues at the increment-level and for ensuring sustainment is adequate to support Mission Threads and Capability Provisioning Activities (CPAS). NECC Service Oriented Architecture (SOA) and the web-enabled approach for providing capabilities to the Warfighter require continuous re-examination of sustainment practices.

Sustainment for fielded capabilities has two categories: one for software, and one for hardware.

For software sustainment:

- The CPMOs have responsibility for sustaining all the CM software throughout the entire enterprise for all CMs assigned to them for development. Section 5 of this document contains individual CPMO software support concepts.
- The JPMO has responsibility for sustaining all the software required for the Federated Development and Certification Environment (FDCE).

For hardware sustainment:

- The CPMOs have responsibility for sustaining all the hardware required for the NECC Local Nodes within their Service/Component.
- The JPMO has responsibility for sustaining all the hardware required for the FDCE.
- The JPMO has responsibility for sustaining all the hardware for the NECC Enterprise Nodes. Section 5 of this document contains the JPMO hardware support concept.

4.3 Basing Concept[7]

The JPMO is responsible for basing the fully-certified CMs (i.e., graduated from the FDCE certification process) at the Enterprise and Local Nodes. For details of the JPMO/CPMO basing requirements, see Basing Concept[8].

4.4 Basing and Deployment Description

The NECC basing concept is to develop and deliver C2 capabilities on the GIG as an integral part of overall GIG operations. All NECC capabilities will be hosted at an existing Defense Enterprise Computing Center (DECC) or similar platform for enterprise use. The Enterprise Nodes will be provisioned by managed service providers as turnkey operations. Local capabilities will be hosted as part of the computing infrastructure at the operational sites determined by the Components. NECC support infrastructure such as the Federated Development and Certification Infrastructure (FDCI), Tier 1 Help Desk, and control center will use existing capacities.

NECC software (and some hardware) will be implemented in various locations around the globe and on multiple platforms. The following table (see Table 1) summarizes the estimated number of NECC locations.

[7] DRAFT NECC CARD, https://gesportal.DoD.mil/sites/necc/milestone_launch/default.aspx

[8] Basing Concept, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Basing Concept.doc

Table 1: NECC Locations

	Sites
Enterprise Sites	**4**
Army Sites	**266**
Army Local Sites	261
Joint Sites	5
Navy Sites	**403**
Afloat	329
Ashore	66
Joint Sites	8
USAF Sites	**350**
USAF Local Sites	342
Joint Sites	8
USMC Sites	**95**
USMC Local Sites	95
Joint Sites	0
DISA Sites	**2**
GRAND TOTAL =	**1120**

4.4.1 Virtualization

Virtualization grew out of a need by IT departments for a simplified deployment environment, and for more efficient use of available servers. It achieves these goals by adding a virtualization layer on top of the underlying platform. This added layer abstracts the hardware and Operating System (OS), thereby providing a uniform and simpler deployment environment. Since the virtualization layer can host multiple virtual machines, it is possible to maximize a server's available resources. For example, relational databases often use only a fraction of a server's Central Processing Unit (CPU), which then sits idle. With virtualization, applications that use that formerly idle CPU can be added, while maintaining true application isolation.

4.4.2 GIG Computing Nodes

GCN bring the benefits of virtualization to the DoD. They establish a common, Joint virtualized server environment into which programs throughout DoD can provision their software (see Figure 1). They also have the potential to function as a universal security and accreditation environment. NECC has adopted the GCN as its target deployment environment.

If required, multiple echelons possess the ability to establish GCNs at fixed, operational, and tactical locations. All NECC GCNs connect to form a network of complementary, distributed, and robust capabilities.

4.4.3 NECC Virtualization Requirements[9]

NECC requires that Local and Enterprise Nodes support a common, virtualized environment. The requirements are as follows:

1. **Hardware**: The hosting computer must use an x86-based CPU. SPARC and PowerPC CPUs are not supported.
2. **Host Operating System**: VMWare ESX Server (VMWare Infrastructure 3.0)
3. **Virtual Machine Software**: VMWare Infrastructure 3.0
4. **Operating System**: Choose one of three - Linux, Solaris x86, or Microsoft Windows
5. **Applications**: CM-specific

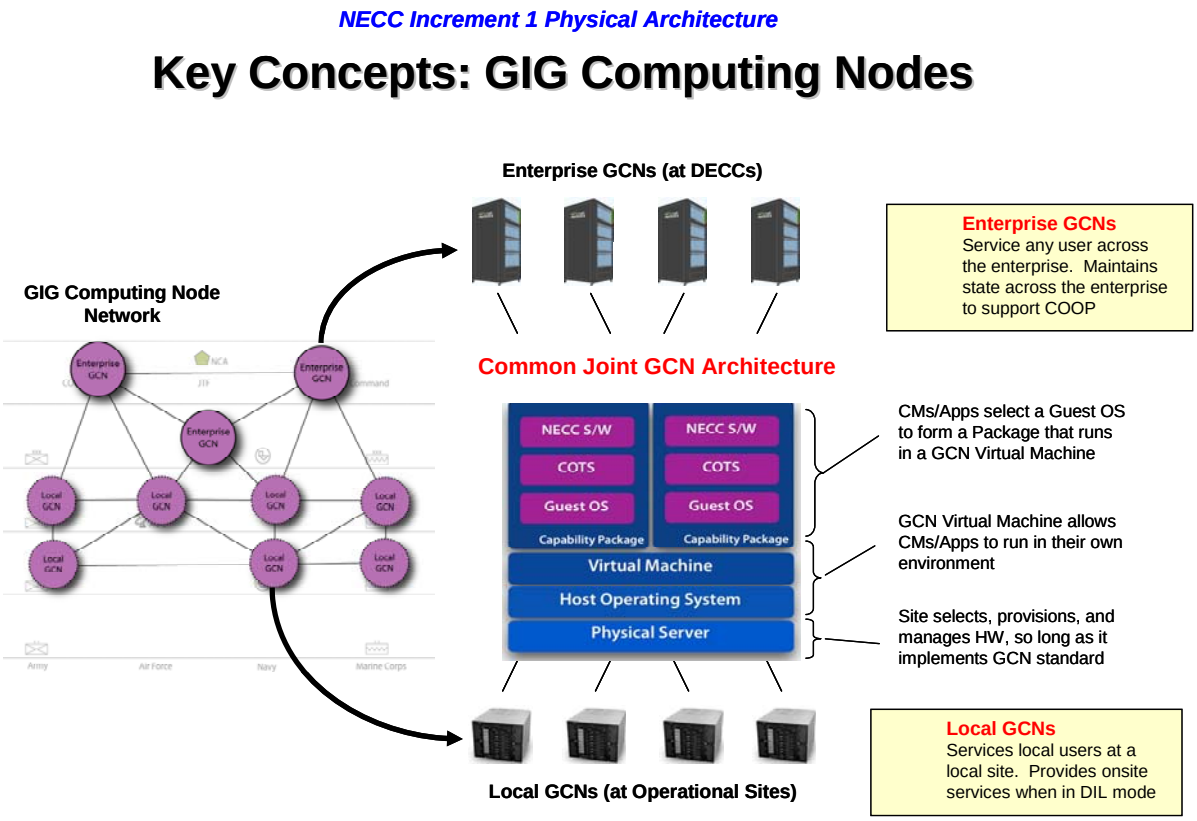

Figure 1: NECC Increment 1 Physical Architecture

For details about the CPMO Basing requirements, ctrl-click **here**[10].

---

[9] NECC Increment 1 Physical Architecture, version 1.2.3, Para 2.1, 23 Mar 2007, https://gesportal.DoD.mil/sites/necc/architecture/Shared%20Documents/Architecture%20Working%20Group%20Products/NECC%20Increment%201%20Architecture%20Description/NECC%20Increment%201%20Physical%20Architecture%20v1.2.3.pdf

[10] Basing Concept, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Basing Concept.doc

4.5 Interfaces and Supporting Systems

The NECC Client Solution selection was thin clients (clients that do as much processing as possible and pass only data for communications and storage to the server), as opposed to thick clients (client computers or client software in client-server architecture networks, which depend primarily on the central server for processing activities, and mainly focus on conveying input and output between the user and the remote server). NECC has no plans to field special-purpose client-hardware devices. The NECC Client Solution selection criteria were (1) the amount of software planned to operate with a web-browser environment (more is better), and (2) the amount of special-purpose software required (less is better).

4.6 Operating Environments

Standards and common service interfaces are a key part of software component design. However, to realize the objective architecture, their design must also take into account the operational environment for which they are intended. A good software component needs a strong technical foundation. This is accomplished by using the right technology and ensuring non-technical requirements meet its environment. Operational environments generally equate to echelon. Tactical echelons have different non-technical requirements from strategic ones; for example, they may need to operate when disconnected from the GIG. Software components must meet the needs of their operational environment and simultaneously maintain alignment with overall NECC goals and priorities, such as interoperability.

The most important aspect of an operational environment is mission-criticality. The term, "mission-critical," represents a capability needed by the Warfighter to execute a primary mission within a given operational environment. Whether or not a capability is mission-critical determines design and deployment considerations of the software components. The Warfighter must have reliable and consistent access to the software components that deliver that capability.

For further details about the CPMO requirements, ctrl-click **here**[11].

4.7 Architecture

NECC's architecture objective is to deliver a single (JC2) architecture for current and future JC2 services and capabilities, implemented in a SOA construct. Transition from today's stovepipe C2 systems to a single Joint-SOA-based architecture is accomplished over several increments, commencing with Increment 1. Each increment develops a specific architecture implementation that moves NECC closer to its objective. The Architecture Framework Document[12] directs an individual Increment's architecture development for NECC. It also establishes the overarching guidance across five key architectural views: physical, software, data, information assurance, and technical operations. Key principles include simplicity, enterprise relevance, service-oriented feature, and leveraging of current C2 systems and operational suitability.

---

[11] Operating Environments, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Operating Environments.doc

[12] Architecture Framework, 31 Jan 2007, version 1.0, https://gesportal.DoD.mil/sites/necc/architecture/Shared%20Documents/Architecture%20Working%20Group%20Products/NECC%20Architecture%20Framework/ARCHITECTURE%20FRAMEWORK%20version%201.doc

4.8 Legacy Systems Implemented in NECC

Further details of CPMO requirements for legacy systems are provided at ctrl-click **here**[13].

4.9 Current GCCS FoS Maintenance and Operational Support Systems

Further details of CPMO requirements for current GCCS FoS systems are provided at ctrl-click **here**[14].

4.10 NECC Maintenance and Operational Support Systems

Managed service providers account for hardware maintenance and support policies. Since the service providers own the equipment, a disposal process for classified information needs to be developed. The amount of equipment disposed depends on the level of classification and the service provider's implementation. Disposal of this equipment may incur an additional cost to the Government if not negotiated ahead of time with the service provider.

The service provider is responsible for software support during development, production, and fielding. Responsibility for post-fielding software support is assessed and determined during the Depot Core Assessment. In the Sustainment lifecycle phase, annual software releases help modify and update system software to correct problems or incorporate recommendations provided by the user. These scheduled releases are closely coordinated with the support systems management effort to maintain consistent baselines.

Software problems/releases are conducted on an as-needed basis to correct pressing or critical problems identified by the gaining units that cannot wait until a scheduled release date. A single point-of-control closely coordinates out-of-cycle, quick-change releases within the support systems management effort. This ensures fluid coordinated releases and configurations control, coupled with timely support to the benefiting units.

4.10.1 NECC Joint Technical Operations Control Capability Concept

The NECC Joint Technical Operations Control Capability (JTOCC) supports application-layer network and systems management, visibility, monitoring, analysis, planning, and control. This capability facilitates the net-centric transformation of NECC-level enterprise services by optimizing integrated network operations of existing and emerging applications networks and services. The TOCC and Help Desk, the two components of the NECC JTOCC, work together in an integrated, seamless fashion to the outside world. Internally, however, the two components focus on different areas. The NECC Help Desk function is outward-facing. It provides a well-known interface point for end-users and is responsible for creating and tracking trouble tickets in response to user requests for general help, or debugging specific problems. The TOCC focuses

---

[13] Existing Systems Implemented in NECC, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Existing Systems Implemented in NECC.doc

[14] Existing GCCS FOS Maintenance and Operational Support Systems, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Existing GCCS FOS Maintenance and Operational Support Systems.doc

on the coordination and control of individual CMs and their associated CM providers. Since a NECC guiding principle use service providers and service consumers, Service Level Management (SLM) principles are critical.

The NECC Help Desk consists of a web-based collaborative Tier 1 environment, and a physical three-tiered environment. The web-based resource allows all users access to NECC capabilities 24/7/365. It provides CM updates, network information, quick fixes, information regarding common problems, virtual meeting places, audio and video over IP, and whiteboard instructions on how to get to the appropriate physical tier-level within NECC. The physical Help Desk implements a three-tier infrastructure using the Standard DoD Priority System for issues with CMs. The JPMO staffs the Tier 1 Help Desk with support personnel. If the first level of support is unable to resolve an issue, or if the issue focuses on a specific behavior of a CM, Tier 1 will redirect a user to the Tier 2 Help Desk of the CPMO responsible for its development. If the second level Help Desk personnel cannot resolve the issue or if the resolution requires modifications to the underlying software of the CM, the problem escalates to Tier 3 (i.e., to the CM developer).

4.10.2 Roles and Responsibilities

4.10.2.1 Joint Program Management Office

The JPMO manages operations in support of the NECC Tier 1 Help Desk. The JPMO facilitates the structure and operating environment (not the CM-specific content) of the web-based collaborative Tier 1 Help Desk. This includes the portal and all applicable updates to the online resource. In the physical Tier 1 environment, the JPMO supports operations of the Multi-CM Dependency Oversight Group located in the JTOCC. The JPMO governs all matters involving CMs, with inputs from CPMOs.

The JPMO uses the Net-Centric Enterprise Services (NCES) Enterprise Collaboration Product Line. It operates a set of web-accessible software that enables GIG users to deliver presentations; view, edit, and graphically annotate documents; share applications; and collaborate in real-time with remote co-workers. The capabilities they provide to the user include: Session Management, Presence and Awareness, Text Collaboration, Audio and Video over IP, Whiteboarding and Annotation, Application Sharing/Broadcasting, and Virtual Spaces.

This resource is available at all levels of local infrastructure for troubleshooting and information-sharing purposes. Updates to common problems and quick fixes are reviewed by CM Subject Matter Experts (SMEs), then, posted to the collaborative environment for the user. Users can also post fixes they have discovered through experience, but the input must be reviewed by a SME to verify the content and avoid malicious information-sharing.

4.10.2.2 Component Program Management Offices

The CPMOs support the operation of CM-specific Tier 2 Help Desk support for each CM under their purview. They also manage input to the Virtual Tier 1 Environment, but not the upkeep of the resource. Each CPMO stations a representative at the JTOCC to monitor and coordinate routine management functions of the CMs under their control. The personnel from DECC-C conduct the actual operation of this function and receive funding from the JPMO. This office coordinates issues involving multiple CM dependencies and cross-CM troubleshooting.

4.10.3 Delivering New or Updated CMs to the Warfighter

The following is a breakdown of the three-step process to deploy and provision CMs into the NECC user community (see Figure 2).

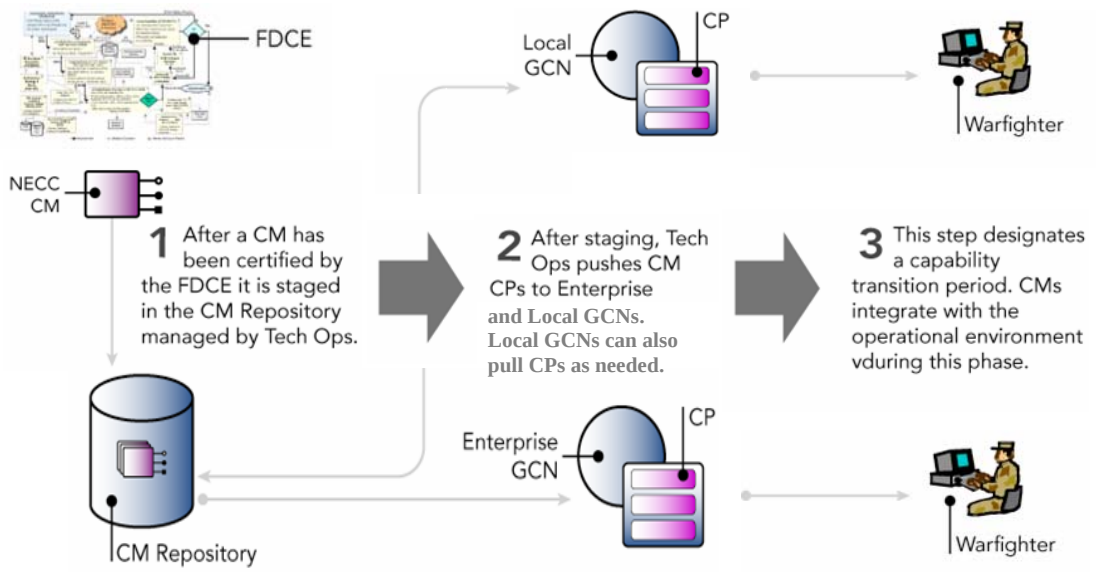

Figure 2: CM Deployment and Provisioning Process

Step 1: This stage describes the process of a CM maturing through the FDCE process into the Operational Piloting Phase. At this time, the NECC JTOCC works directly with the FDCE to mature the capability to an Operationally Ready status, at which time the JTOCC coordinates with the Enterprise GCN for migration.

Step 1a: A CM matures into the Operational Piloting Phase of the FDCE process as it becomes GIG-compliant in the areas of Certification and Accreditation (C&A) and Net-readiness. Once it achieves phase one certification, the CM moves into the second stage of step one.

Step 1b: The CM is then deposited into the CM repository, located at the JTOCC. During this time period, the CM has already been certified and accredited to operate on the GIG by the FDCE. This portion of the process will take place during the Operational Piloting Phase of the FDCE process. Starting the process here allows for an easier transition into the Operational Phase. The JPMO will verify that the CM Support Packages have been populated to the CM Support Infrastructure (Help Desk Troubleshooting Tools, Web-Based Collaborative Tier 1 Environment, Configuration Management, etc.). The CM is then migrated to the appropriate Enterprise-level GCN DECC, where it begins step 2, and the deployment process.

- The JTOCC will comply with current DOD JTF–GNO reporting procedures and information dissemination into the NetCop provided by the Global Infrastructure Service Management Center (GISMC). The JTOCC also interfaces with DNCs, such as the Global NetOps Support Center (GNSC) and the Theater NetOps Centers (TNC), which support JTF–GNO operations in COCOM-specific GIG Areas of Responsibility (AoR). All reporting will be done in accordance with current JTF–GNO GIG reporting procedures.

Step 2: This stage describes the process of a CM being deployed into the Enterprise-level and Local-level GCNs. The CM is deployed to the Enterprise and Local GCNs. The CM is updated into the NetCop, coordinates with GISMC for procedural issues and compliance, and verifies provisioning status (e.g., did it arrive? Does it work?) and provision-level. Local GCNs are responsible for providing an operating area-specific NetCop to the Enterprise GCN, to be rolled up into a total NetCop, which is then provided to the JTF–GNO via the GISMC.

Step 3: This stage describes the process by which the user will use the CM after provisioning.

Step 3a: During the Capability Transition Period (CPT), the user registers with the CM. This is the period of time in which the user or Warfighter begins the process of training the new CM, supporting the new CM, integrating the new capability with current capabilities, and conducting exercises to show Proof-of-Concept and Operational Effectiveness. The amount of time for this stage will be different for each Service component, but a specific threshold, decided by the use of different types of metrics, should be established to identify if CMs being provisioned are not being used and why.

Step 3b: During the Operational Use stage, the user actively engages the new CM to support the warfighting mission.

4.10.4 NECC Help Desk Tiered Structure

The following describes the process a user goes through to access the different Help Desk resources and Tier structures for troubleshooting purposes. Technical support happens through various media including e-mail, live chat, telephones, applications, faxes, and technicians. However, the most common method of support is typically via a telephone.

4.10.4.1 Tier 1 Support

The user enters Tier 1 after verifying the issue does not involve, or is caused by, local communications network issues or applications. The support staff members provide entry-level assistance, 24/7/365, by opening a trouble ticket with the REMEDY TMS central database. Then, it enters basic information from the user (unit, service, application, location, etc.) into the Trouble Management System (TMS) by using CM support tools for basic troubleshooting (question checklists, common problems, and quick fixes) and triage processes. If the operator can fix the issue at this point, the ticket will be closed and documented for performance tracking purposes. If the issue cannot be resolved at the Tier 1 level, the operator will escalate the issue, based on standard DoD Priority Reporting Procedures, to the appropriate Tier 2 SME.

Users can also access the Tier 1 Help Desk via the Web-based Collaborative Tier 1 Environment. Users can access menus, question checklists, common problem pages, quick-fix processes, and other resources to solve issues. If the issue cannot be resolved, the web resource will direct the user to the NECC Tier 1 Help Desk, where a trouble ticket will be opened for the issue.

4.10.4.2 Tier 2 Support

Tier 2 support will be provided on a 24/7/365 basis for operations. It will consist of operators that are SMEs within certain CMs, and can provide higher levels of support. This level will deal with specific NECC applications or systems issues, hardware support, and network management.

The operator will receive the trouble ticket from the Tier 1 group, assess the priority of the issue, and coordinate with support staff members to diagnose the problem. If the Tier 2 personnel cannot solve the issue, they will escalate the ticket to the Tier 3 group.

Users may access the Tier 2 Help Desk directly, depending on the issue at hand. Also, the Tier 2 Help Desk might contact the user to assist in troubleshooting the problem. Guidance to access the Tier 2 directly can also come from the Web-based Collaborative Tier 1 Environment.

4.10.4.3 Tier 3 Support

Tier 3 consists of specialized support, which is typically higher-level engineers and/or program or systems developers. This level of support is not 24/7/365. The support staff members at this level work a normal M-F, 9-5 workday, but are available on-call after hours 24/7/365. Tier 3 personnel will receive trouble tickets via the REMEDY TMS and work the issues based on the priority classification.

4.10.5 JTOCC

The JTOCC serves as the high-level connection source to receive all CM Enterprise Service Management (ESM) reports. The main function of CM management is Runtime Governance, which consists of SLM and SLA enforcement. It will serve as the clearinghouse for reporting statistics, compliance with SLAs, and availability performance metrics. The focus of a JTOCC in the SLM function is to aggregate the results of ESM reports from the various CM providers, and provide solid metric information on issues such as quality of service, SLA enforcement, and all the other SLM disciplines. The JTOCC will also maintain a close relationship with the NECC Help Desk infrastructure, as well as DNCs for Network Situational Awareness and NetCop reporting guidelines.

4.10.6 NECC-wide Runtime Governance

The distributed and heterogeneous nature of these evolutionary, service-based CMs raises governance issues throughout the operational phase of the product lifecycle. To gain the full benefits of SOA, runtime governance will address a specific set of requirements, which include, but are not limited to:

- Supporting service, CM, and system-wide security concerns through logging, authentication, and authorization functions
- Providing insight into CM interactions, as well as the overarching business transactions and processes
- Managing and maintaining service levels
- Managing errors and exceptions
- Enabling online upgrades and versioning
- Validating updated CMs before redeploying them into production
- Auditing, logging, and diagnosing systems in production

A Runtime Validation System enables operations teams to verify the functionality and performance of new or modified CMs, in support of runtime governance policies and processes. An effective validation system provides the following:

- Validates individual services against the entire set of dependent CMs
- Monitors and reports metrics for CMs or individual services, which includes service availability, response time, fault tracking, and throughput
- Uses message capture across diverse environments to incrementally measure and report on the performance and functionality of web services and CMs
- Provides real-time, easy-to-digest performance charts and searchable message logs
- Analyzes performance bottlenecks and errors
- Inspects SOAP messages for content, faults, and errors
- Resubmits messages from history or auto-generates new Simple Object Access Protocol (SOAP) messages to fine-tune web services
- Creates service and/or CM dependencies and provides correlation mapping

4.11 Resources Required to Support Existing GCCS FoS Systems

The Services/Components are required to sustain existing GCCS FoS capabilities during the transition from GCCS FoS to NECC, until the transition to NECC is complete. For further details about the CPMO/Components requirements, ctrl-click **here**[15].

4.12 Resources Required to Support Proposed NECC Systems

4.12.1 Net-Centric Enterprise Services

NECC is net-centric based. In other words, it is a networked collection of capabilities empowering the user to pull required information from any available source, with minimal latency. NECC's net-centric capabilities reside on the Core Enterprise Services (CES). CES provides and manages the underlying net-centric capabilities to deliver content and value to end users.

NCES provides the vehicle for net-centric enterprise services as the basis for the cross-functional capabilities supporting NECC and Service-unique applications and information services. NECC users utilize NCES based on GIG Enterprise Services (GES) to access Service/Agency/Joint-provided Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) services and data sources. NECC architecture supports secure vertical/horizontal information exchange between elements of the NECC community, NGOs, and SMEs.

NECC integrates databases, servers, client workstations, Local Area Networks (LAN), and computer software into an open, scalable, network-centric single architecture, while maintaining compliance with Net-Centric Operations and Warfare Reference Model (NCOW RM), Net-

---

[15] Resources Required to Support Existing GCCS FoS Systems, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Resources Required to Support Existing FoS Systems.doc

Centric Data Strategy (NCDS), NCES, and the DoD IT Standards Registry (DISR). CES is a key component of GES, which is a collection of net-based capabilities composed of networks, the core services, and Community of Interest (COI) services. The NCES program incrementally delivers the CES. NCES is a DISA program intended to implement key enabling capabilities for net-centric operations. NCES provides a common set of interoperable information capabilities in the GIG to access, collect, process, store, disseminate, and manage information on demand for Warfighters, policy makers, and support organizations.

A key enabler for planning and decision-making is the establishment and use of a collaborative information environment (CIE). NCES provides the CIE and information-sharing backbone to NECC users. This provides Warfighters an environment to exercise enhanced organizational effectiveness and reduce hierarchical, serial-planning timelines through information/idea-sharing and parallel planning.

A further NECC NCES discussion is given in the CDD[16] on Para 1.5.

5 INTEGRATED LOGISTICS SUPPORT

Supportability is accomplished by addressing the ten core logistics elements. These are maintenance planning; supply support; support and test equipment; manpower and personnel; training and training support; technical data; computer resources; facilities; packaging, handling, storage, and transportation; and design interface.

5.1 NECC Maintenance Planning

5.1.1 NECC Hardware

NECC incorporates emerging hardware technologies. NECC provides a net-centric environment by introducing PC workstations running on an architecture that has commonality with Joint Command, Control, Communications, Computer, Intelligence Surveillance, and Reconnaissance (C4ISR) systems, delivering tools to promote collaboration among users, and utilizing databases that connect across the Joint community.

NECC uses an evolutionary acquisition strategy, rapid prototyping, extensive user involvement, and integration of Commercial-Off-the-Shelf (COTS) and Government-Off-the-Shelf (GOTS) components. NECC also uses some existing hardware and is upgrading to new hardware for Enterprise and Local Nodes to support integration in garrison or mobile environments. Integration and fielding of NECC hardware upgrades is accomplished with minimal disruption to operational and support missions. Managed service providers provide hardware or software maintenance and support policies.

The NECC Site Architecture Framework (see Figure 3) allows for Capability Nodes to be deployed to sites with their own dedicated hardware suites. Capability Nodes are packaged together on NECC-provided hardware suites (NECC Physical Capability Node Packages), or installed and operated on site-provided hardware (NECC Logical Capability Node Packages).

---

[16] NECC CDD, 6 Feb 2007, https://gesportal.dod.mil/sites/necc/Documents/default.aspx?RootFolder=%2fsites%2fnecc%2fDocuments%2fShared%20Documents%2fCapability%20Development%20Document%20%28CDD%29%20Archive&View=%7bF11F413D%2d5519%2d4735%2d8682%2d97E3776210E0%7d

5.1.2 NECC Capability Nodes

NECC Capability Nodes are deployed as self-contained sets of hardware and software. They have a number of attractive attributes, the most important being that these nodes avoid the complications of having to work through integration issues to coexist with other Capability Nodes in a shared hardware environment. NECC Capability Nodes plug into the LAN sites, which minimize the amount of site integration required. In addition, because they are self-contained, NECC Capability Nodes provide the least amount of additional security accreditation requirements. The use of NECC Capability Nodes is most feasible for Enterprise Capability Nodes where (1) the space and power constraints of the site are at a minimum, and (2) the expected service demand is likely to be sufficiently high to warrant a dedicated hardware suite. At forward NECC sites where space and power is more limited, it may not be practical to deploy Capability Nodes. In such cases, they deploy as either a Physical or Logical Capability Node Package.

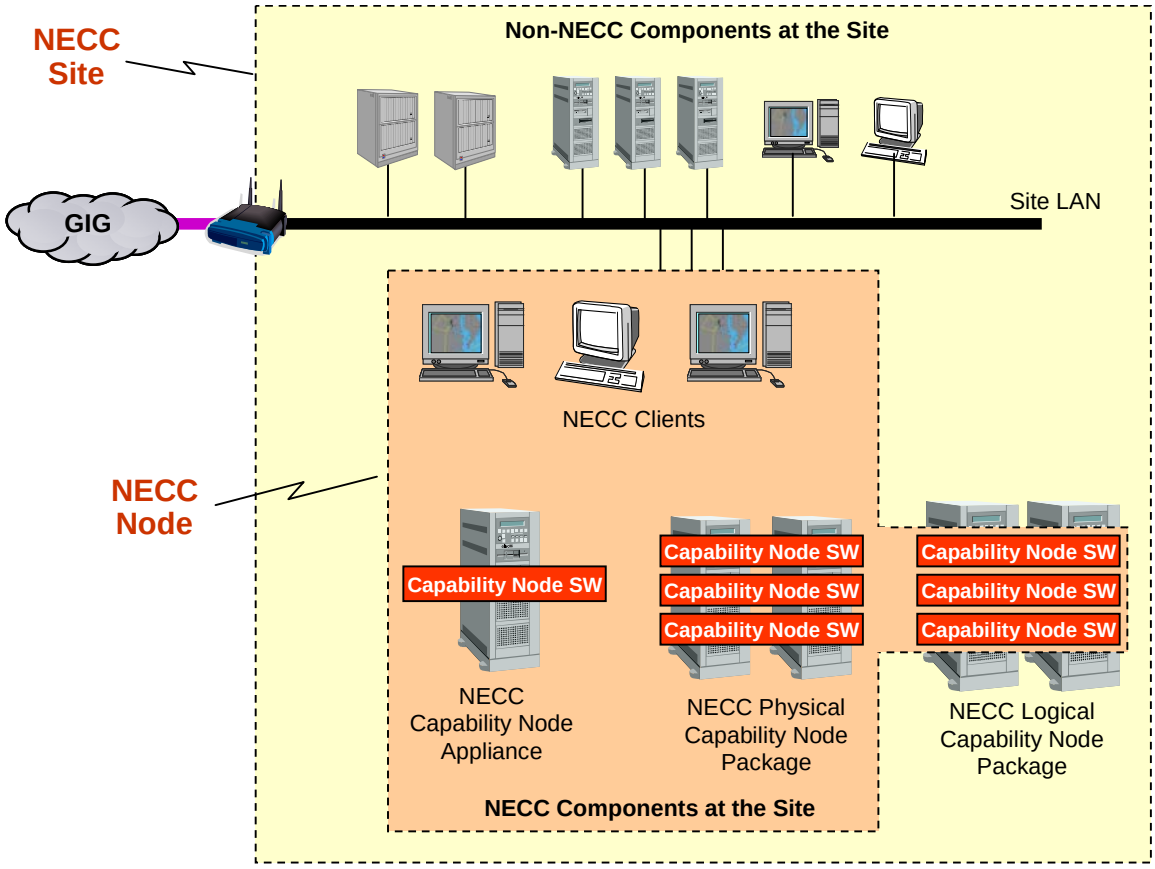

Figure 3: NECC Site Architecture

The NECC Physical Architecture Framework allows for two modes of operation –Remotely Supported Sites (where consumers access and run NECC-provided capabilities across the GIG) and Locally Supported Sites (where consumers access and run NECC capabilities from within their own site).

5.1.3 NECC Remotely Supported Sites

NECC Remotely Supported Sites (see Figure 4) use NECC capabilities that are resident at NECC Enterprise Sites. NECC Remotely Supported Sites have a number of advantages over NECC Locally Supported Sites, including: (1) footprint at the site (space, power, etc.); (2) site integration costs; (3) site administration burden; and (4) site operating and sustainment costs. However, NECC Remotely Supported Sites also have a number of disadvantages, including: (1) no ability to support Disconnected/Intermittently connected/Limited connectivity (DIL) operations; (2) lower performance (in most cases); and (3) no ability for site-specific policy control.

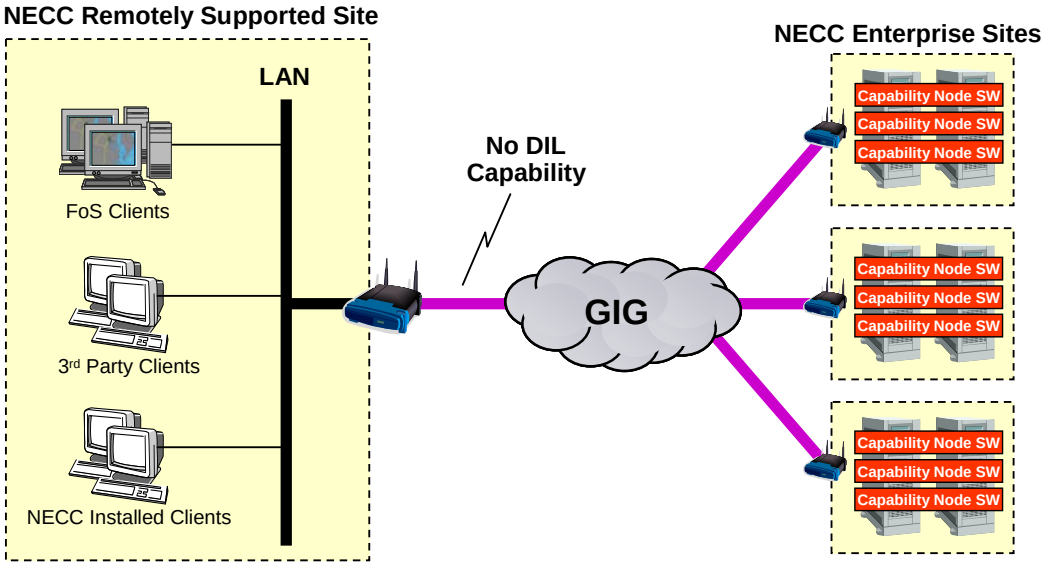

Figure 4: Remotely Supported Site

5.1.4 NECC Locally Supported Sites

NECC Locally Supported Sites (see Figure 5) use NECC capabilities hosted at the local site that provide capability even when the site is disconnected from the GIG. NECC Locally Supported Sites have a number of advantages over NECC Remotely Supported Sites, including: (1) the ability to support DIL operations; (2) improved performance (in most cases); and (3) the ability for local policy controls. However, NECC Locally Supported Sites also have a number of disadvantages, including: (1) non-zero footprint at the site; (2) higher site integration costs; (3) non-zero site administration costs; and (4) non-zero operating and sustainment costs.

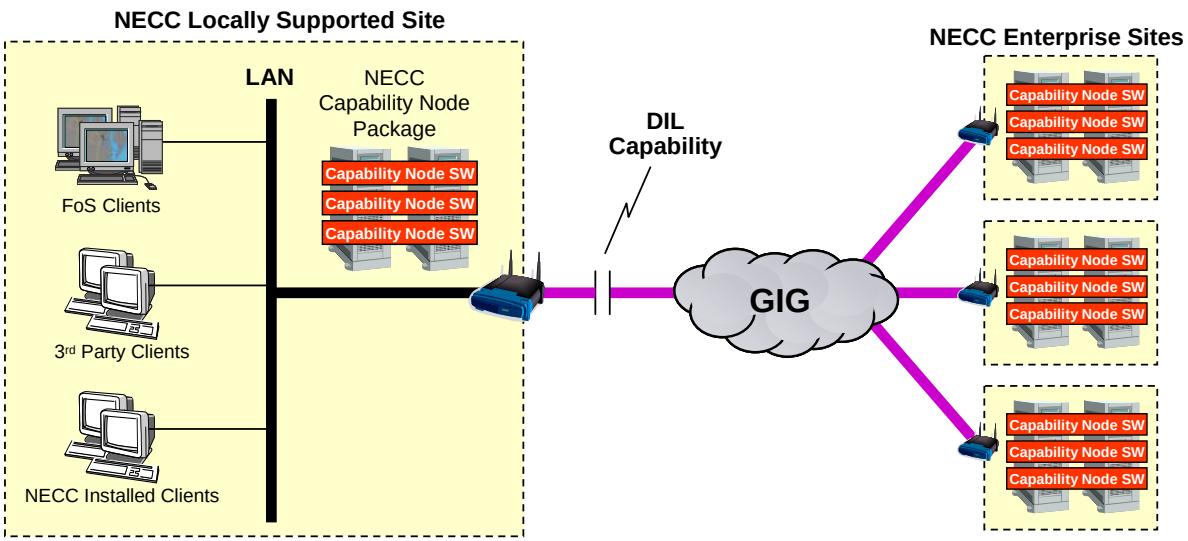

Figure 5: Locally Supported Site

For further details about the CPMO/Components requirements, ctrl-click **here**[17].

5.1.5 NECC Software

The CPMOs manage the NECC Support Concept for externally hosted CM Government software and hardware. A CPMO establishes permanent hosting locations, maintenance agreements, and Help Desk support for the participating CMs. SLAs between the JPMO and CPMO offices define the specific terms of hosting and support requirements for each CM.

Responsibility for post-fielding software support is assessed and determined during the Depot Core Assessment. Support for each CM is allocated to the CPMO responsible for development.

Resolution of software problems is accomplished on an as-needed basis. Releases will be closely coordinated within the support systems management effort to ensure timely, coordinated release, and configuration control.

To support evolutionary growth, NECC is designed to ease platform portability, promote smooth integration of new applications, and facilitate supportability. CPMO-provided software applications are considered as candidate solutions to meet NECC Mission Capability Package (MCP) requirements. NECC software (e.g., COTS, GOTS, and new development) must comply with and support industry and DoD standards for open systems. NECC MCPs must comply with Joint Technical Architecture (JTA) and applicable DoD Information Assurance (IA) security requirements to ensure interoperability and compatibility with required GIG C2 systems and communications networks. To ensure interoperability with existing service systems, NECC software must provide backwards-compatible with COE 4.X-compliant (Common Operating Environment) service variants.

For further details about the CPMO/Components requirements, ctrl-click **here**[18].

---

[17] NECC Maintenance Planning, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/NECC Maintenance Planning.doc

5.1.6 FDCE Hardware and Software Support

The JPMO sustains the hardware and software required for FDCE operations. This includes capabilities for the FDCE portal, as well as capabilities provided by other organizations, such as the CPMOs, JITC (Joint Test Interoperability Command), JMETC (Joint Mission Environment Test Capability), OTAs (Operational Test Authorities), etc., that are accessed to provide FDCE capabilities.

The JPMO sustains the hardware and software required to maintain the FDCE portal. The organizations providing other capabilities will be responsible for sustaining them. The JPMO establishes SLAs with each organization for these activities.

5.2 Supply Support

NECC's Supply Support Strategy uses existing commercial support, whereby each vendor provides the necessary supply support (e.g., spares, tools, and test equipment) required for the repair of failed items. The JPMO has responsibility for Supply Support of the NECC Operations Center and the Enterprise Nodes. The CPMOs have responsibility for the Local Nodes under their purview. For further details of the individual Components' supply support policies, procedures, and requirements, ctrl-click **here**[19].

5.3 Support and Test Equipment

NECC maintenance and system administration personnel will not require any Peculiar Support Equipment (PSE). Test and fault isolation capabilities of support equipment shall meet performance levels consistent with NECC reliability and maintainability standards. NECC shall meet the industry standard for Mean-Time-Between-Essential-Function-Failure. The JPMO has responsibility for the acquisition, development, and/or sustainment of Support Equipment for the NECC Operations Center and the Enterprise Nodes. The CPMOs have responsibility for the acquisition, development, and sustainment of Support Equipment for the Local Nodes. For further details of the CPMO/Components requirements, ctrl-click **here**[20].

5.4 Manpower and Personnel

Proper manning requires identifying and acquiring personnel with skills required to operate and maintain NECC over its lifetime. The NECC operational manpower concept characterizes the workload into the following categories:

1. Operators – Personnel who use NECC to perform their primary duties
2. Supervisors – Personnel who supervise the operation of NECC to support command objectives

---

[18] NECC Maintenance Planning, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/NECC Maintenance Planning.doc

[19] Supply Support, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Supply Support.doc

[20] Support Equipment, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Support Equipment.doc

3. Administrators – Personnel who set and maintain NECC system functionality, database parameters, and configurations within their operational commands
4. Technicians – Personnel who perform maintenance tasks on NECC hardware and supporting infrastructure within their operational commands
5. Employment Planners – Personnel who plan and direct the use of existing C2 systems and promote needed capabilities in new C2 systems

The following table (see Table 2) provides the approximate operational manpower required for NECC.

Table 2: Approximate Operational Manpower Requirements

	Operators	Supervisors	Administrators	Technical	Employment Planners
Army Local Nodes	**803**	**0**	**449**	**0**	**0**
Navy Local Nodes	**2,319**	**0**	**531**	**571**	**0**
Air Force Local Nodes	**20,564**	**0**	**1645**	**0**	**0**
USMC Local Nodes	**297**	**0**	**0**	**0**	**0**
DISA Local Nodes	**575**	**0**	**14**	**0**	**0**
JTF HQ	**364**	**798**	**25**	**22**	**0**
Total	24,922	798	2,664	593	0

The Joint Program Executive Office (JPEO) established the NECC JPMO to oversee the development of the NECC program strategy, architecture, system engineering, and migration plans to move C2 systems from current architectures to a net-enabled capability. The NECC JPMO is responsible for articulating the program objective. The total NECC Program Management organization follows (see Figure 6).

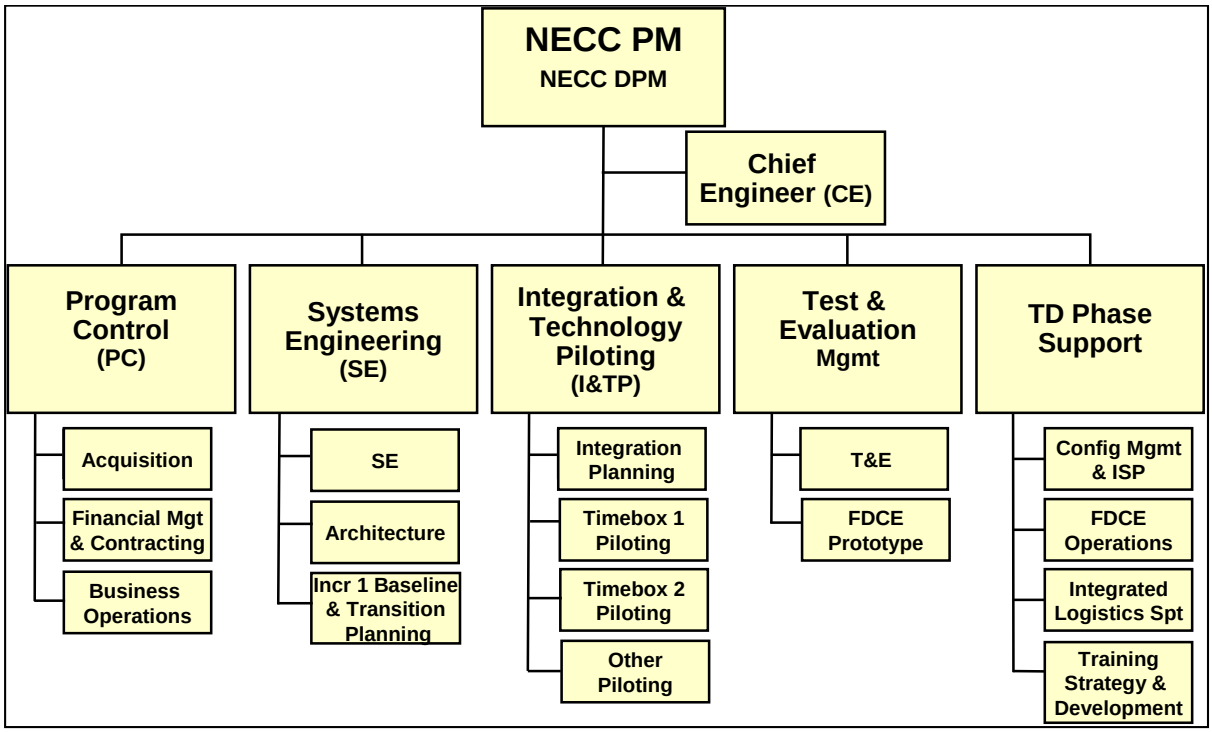

Figure 6: NECC JPMO Organization

5.5 Training and Training Support

The JPMO has responsibility for Training and Training Support for the NECC Operations Center, the NECC Help Desks at Tiers 1 and 3, and the Enterprise Nodes. The CPMOs have responsibility for the Local Nodes and Tier 2 Help Desks under their purview. For further details about the CPMO/Components requirements, ctrl-click **here**[21].

5.6 Technical Data

Technical data is recorded information of a scientific nature, and includes manuals, drawings, parts lists, change notices, system software documentation, and other technical publications related to the installation and operation of a system (e.g., specifications, standards, engineering drawings, database schemas, task analysis instructions, data item descriptions, reports, and equipment publications).

NECC will be fully supported by technical data. The documentation will accurately describe how to use and support NECC. Operations manuals will be available online, searchable, and printable as required.

NECC technical data will be required for the following areas:

- CM
  - Operations manuals specific to the CM

[21] Training and Training Support, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Training and Training Support.doc

  - Hosting infrastructure maintenance manuals
- Enterprise Nodes
  - Operations manuals for Enterprise Node infrastructure
  - Maintenance manuals for hardware infrastructure
- Local Nodes
  - Operations manuals for Local Node infrastructure
  - Maintenance manuals for hardware infrastructure
- FDCE Nodes
  - Operations manuals for development, testing, and analysis tools
  - Operations manuals for modeling and simulation tools
  - Technical manuals for C&A tools
- NECC Operations Center
  - Technical manuals associated with operation of the Ops Center
  - Maintenance manuals for hardware infrastructure

5.7 Computer Resources

The JPMO has responsibility for ensuring Computer Resource Support for the NECC Operations Center and the Enterprise Nodes, whether through SLA or organic support. The CPMOs have responsibility for ensuring Computer Resource Support for the Local Nodes under their purview. For further details about the CPMO/Components requirements, ctrl-click **here**[22].

5.8 Facilities

The CPMOs have responsibility for Facilities of Local Nodes under their purview. The JPMO is not responsible for Facility requirements, as current facilities are sufficiently available to support the NECC Operations Center and the Enterprise Nodes. For further details about the CPMO/Components requirements, ctrl-click **here**[23].

5.9 Packaging, Handling, Storage and Transportation (PHS&T)

The JPMO is not responsible for PHS&T. The CPMOs have responsibility for any unique requirements for the Local Nodes under their purview. For further details about the CPMO/Components requirements, ctrl-click **here**[24].

---

[22] Computer Resource Support, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Computer Resource Support.doc

[23] Facilities, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Facilities.doc

[24] Packaging, Handling, Storage and Transportation (PHS&T), 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Packaging.doc

5.10 Design Interface

The JPMO satisfies all Design Interface requirements through SLAs for the NECC Operations Center and the Enterprise Nodes. The CPMOs satisfy all Design Interface requirements for the Local Nodes under their purview. For further details about the CPMO/Components requirements, ctrl-click **here**[25].

6 DETERMINATION OF LOGISTIC RESOURCE REQUIREMENTS

Supportability is a design characteristic. The early focus of Situational Awareness (SA) should result in the establishment of support-related parameters or specification requirements. These parameters should be expressed both quantitatively and qualitatively in operational terms and specifically relate to systems readiness objectives and the support costs of the system. Achieving and sustaining affordable system supportability is a lifecycle management activity and is the result of sound SE. SAs are a wide range of related analyses that should be conducted within the SE process. The goals of SA are to ensure that supportability is included as a system performance requirement and that the system is concurrently developed or acquired with the optimal support system and infrastructure.

As part of the acquisition strategy discussed in the DAG Section 2.3, the Program Manager develops and documents a PSS for lifecycle sustainment and continuous improvement of product affordability, reliability, and supportability, while sustaining readiness (see DAG Section 5.4.1.2.1). This effort ensures that system support and lifecycle affordability considerations are addressed and documented as an integral part of the program's overall acquisition strategy. The PSS defines the supportability planning, analyses, and trade-offs conducted to determine the optimum support concept for a materiel system and strategies for continuous affordability improvement throughout the product lifecycle. The support strategy continues to evolve toward detail, so that by Milestone C, it contains sufficient detail to define how the program will address the fielding and support requirements that meet readiness and performance objectives, lower Life Cycle Cost (LCC), reduce risks, reduce logistics footprint, and avoid harm to the environment and human health. The PSS should address all applicable support requirements, which include, but are not limited to, the following elements:

- Product Support (including software) (DAG Section 5.1.3.1)
- Interoperability (DAG Section 5.1.3.2)
- Data Management (DM) (DAG Section 5.1.3.3)
- Integrated Supply Chain Management (DAG Section 5.1.3.4)
- Life Cycle Cost Optimization (DAG Section 5.1.3.5)
- Logistics Footprint Minimization (DAG Section 5.1.3.6)
- Life cycle Assessment (DAG Section 5.1.3.7)
- Demilitarization and Disposal (DAG Section 5.1.3.8)
- Environment, Safety, and Occupational Health (ESOH) (DAG Sections 5.2.1.6 and 4.4.11)

---

[25] Design Interface, 24 April 2007, https://gesportal.DoD.mil/sites/necc/ILS/ILSSWG/Shared Documents/LSA Links/Design Interface.doc

- Human Systems Integration (HSI) (DAG Section 5.2.1.6 and Chapter 6)
- Review and update the Designated Science and Technology Information
- Review and update the Security Classification Guide
- Review and update the Counterintelligence Support Plan (see DAG Section 5.1.3)

SA, when conducted within the SE process, form the basis for decisions on the scope and level of logistics support, and of equal importance, they lead to performance requirements in the system specification, thus influencing design considerations. The analyses, like the SE process, are ongoing throughout the development cycle in iterative fashion. The initial analyses should focus on the relationships of the evolving operational and readiness requirements, planned support structures, and comparisons with existing force structure and support posture. SA can include any number of tools, practices, or techniques.

NECC does not have any unique data, facility, special packaging, handling, or transportation needs in garrison or deployed environments. NECC components will be transportable worldwide by commercial and military airlift, sealift, and ground transportation. NECC preventive maintenance is limited to tasks and schedules consistent with mission performance needs provided in established planned maintenance systems at each site.

Army

NECC is a software-intensive program. The hardware for NECC will be COTS computer equipment. In accordance with AR 700-127, "The traditional approach to influencing design to minimize support requirements is not generally available for commercial and Non-Developmental Items. Commercial support systems will be utilized to the maximum extent possible, taking into consideration cost, readiness, and wartime sustainability.[26]" Based on this direction, SA for the COTS computer equipment focuses on vendors' reliability data, ease of use, preventive maintenance checks, and services and vendors' warranty support concepts. For example, the Army has several major computer equipment vendors that have agreements with Tobyhanna Army Depot, allowing the Depot to perform warranty maintenance repairs. This proves to be beneficial for 24/7 operational availability when systems are deployed to a contingency location.

The maintainability of the NECC software must be considered in the software design. Software development should be based on a modular design for ease of software maintenance.

Navy

Logistics support concepts should also be addressed regarding remote, physical, and software support.

Remote Support

- In this mode, a site uses NECC as a remote service only.
- The site connects to NECC capabilities across the WAN.
- The site has no NECC hardware or software.

---

[26] AR 700-127, Integrated Logistic Support, 19 Dec 2005 http://www.army.mil/usapa/epubs/pdf/r700_127.pdf

Physical Support

- In this mode, a site uses NECC as a local service.
- The site connects to NECC capabilities across the LAN.
- The site has NECC hardware and software.

Software Support

- In this mode, a site uses NECC as a local service.
- The site connects to NECC capabilities across the LAN.
- The site has NECC software (no hardware).

6.1 Supportability as an Integral Part of the Systems Engineering Process

A key to achieving these supportability goals is an effective application of the SE process. In order to be effective, SA need to be integral to each segment of the SE process (e.g., the Requirements Analysis, Functional Analysis/Allocation, and Synthesis, and Systems Analysis and Control). In order to be effective, SA should be conducted within the framework of the SE process. The lifecycle phases established by the defense acquisition process provide a suitable structure for managing the development, production, and operational support of a total system. The SA conducted within any acquisition phase should be properly aligned with the specific objectives of that phase as defined by the acquisition program needs.

A strategy for performing SE activities should be developed early in the program by the performing organization. As such, selected SA should be identified as input to the SE strategy. The SA input should be an integral part of the program's SE strategy. The strategy input should identify and give the rationale for the inclusion or exclusion of specific analyses. Each activity that is included should be assigned to an organization responsible for its conduct.

SA should be scoped to the objectives and level of design anticipated. The strategy should address all SA needed to analyze, define, and verify supportability thresholds and objectives for a system, and assess the risks in accomplishing the thresholds and objectives. SAs are part of the SE process, as systems engineers are the individuals who frequently conduct SA.

6.2 Supportability Analyses Process

The Supportability Analyses Process follows (see Figure 7). The main parts of supportability include: Maintenance Planning; Spares; Training; PHS&T; Personnel; Technical Data; Tools and Support Equipment; Facilities; and Computer Resources Support.

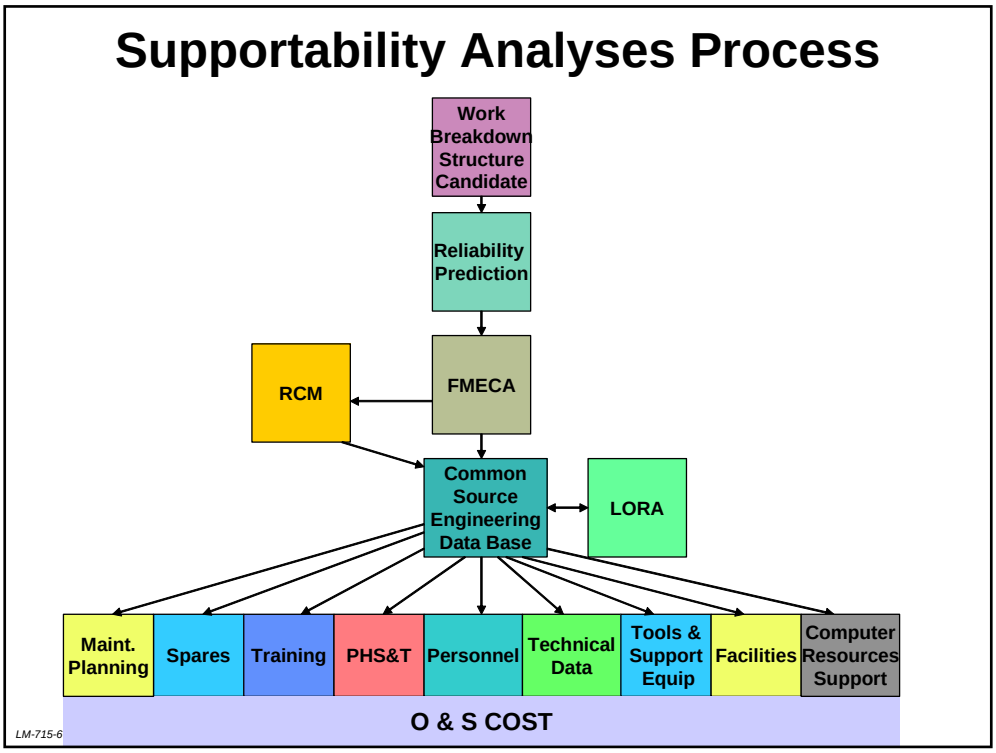

Figure 7: Supportability Analyses Process

There are numerous SA processes. The scientific method process and the nine-phase decision process follow (see Figure 8).

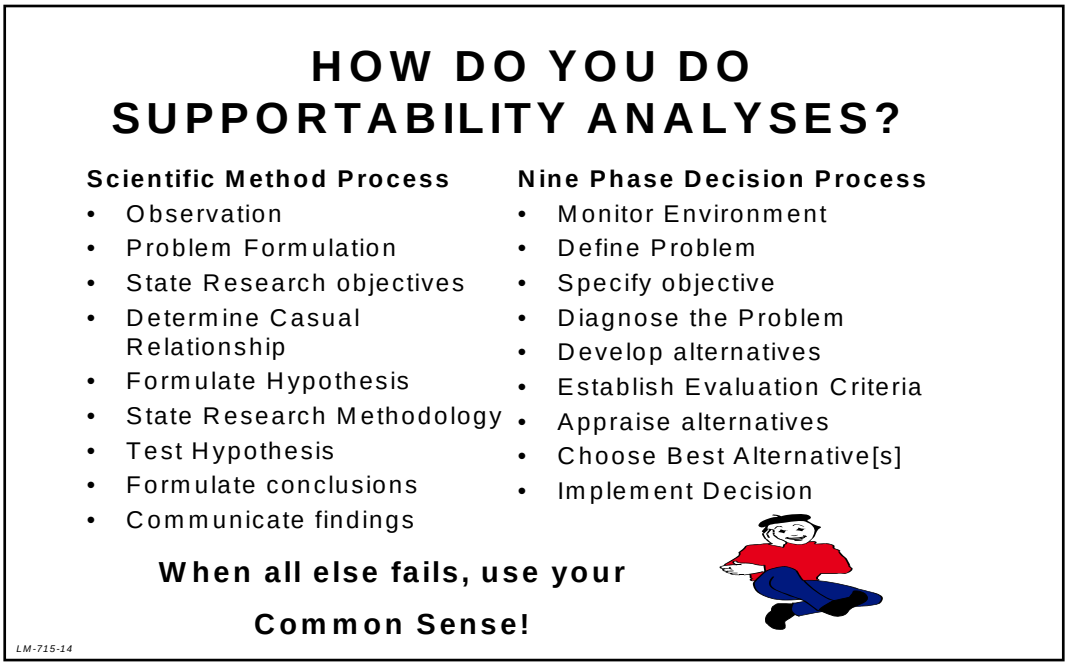

Figure 8: How Do You Do Supportability Analyses?

Additionally, the integrated analyses can include any number of tools, practices, or techniques to realize the goals.

6.3 SA Concepts throughout the Life Cycle

SA includes technical reviews, modeling and simulation, and demonstration and testing. All support performance requirements should be tested and verified.

6.4 Supportability Analyses Reports

Some SA activities (see Figure 9), such as the definition of intended use, are most appropriately executed early on and upfront, while others, such as post-production SA, are best executed subsequent to the initial phases.

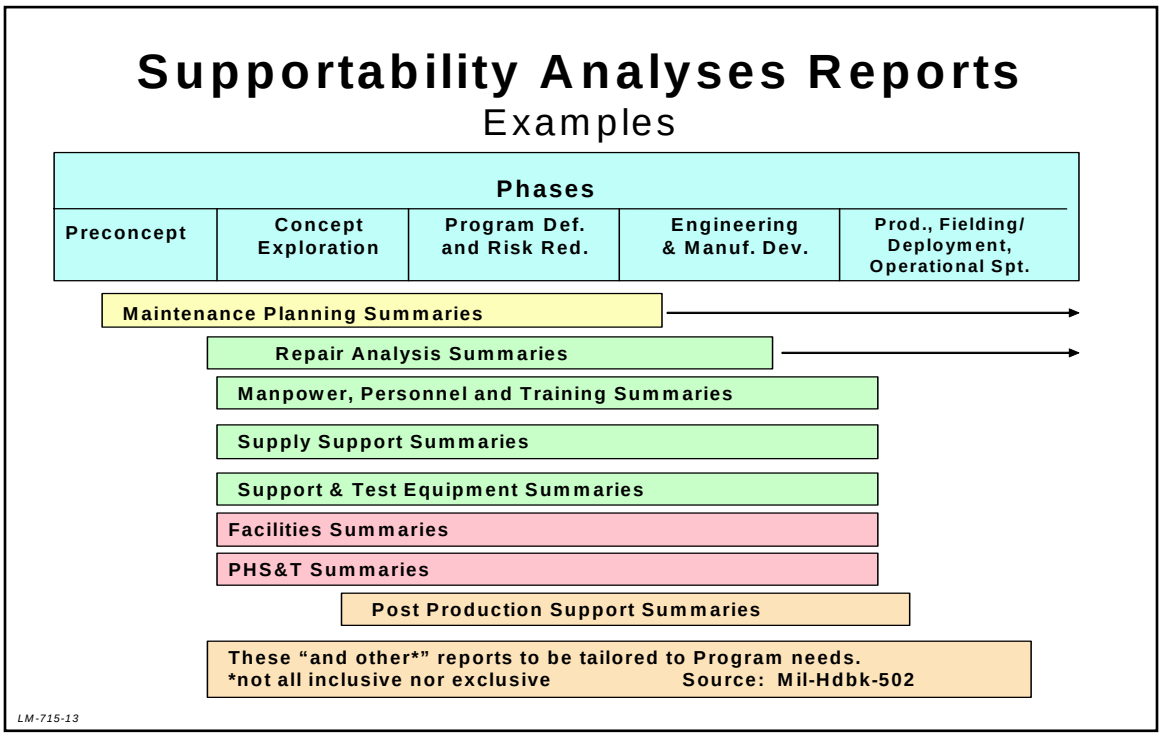

Figure 9: Supportability Analyses Reports

Maintenance Planning Summaries provide maintenance planning information that may be used to develop initial fielding plans for the end item's support structure. These summaries may also be used to verify that the maintenance actions and support structure are aligned with the Government's requirements and maintenance concept.

Repair Analysis Summaries provide conclusions and recommendations of the repair-level analysis. The Government may verify the conclusions and recommendations by using contractor's inputs to perform an in-house analysis.

Manpower, Personnel, and Training Summaries provide information to the Government, so it can establish training plans and ensure manpower and personnel meet applicable constraints. Downsizing in the services causes an even greater concern in the area of HSI. These summaries

identify personnel skills required to perform maintenance tasks, any training required for these tasks to be performed, and manpower estimates at the maintenance-level.

Supply Support Summaries provide the static and application-related hardware information used to determine initial requirements and cataloging of support items procured through the provisioning process.

Support and Test Equipment Summaries provide data necessary to register, or verify the registry of, the support or test equipment in the Government's inventory. They may provide technical parameters, give details of the Test Measurement and Diagnostic Equipment (TMDE) calibration procedures, and list any piece of Category III support equipment needed to maintain the required system's support equipment.

Facilities Summaries identify the facilities required to maintain, operate, and test an item, and train personnel in its use. The facilities may be test, organizational, intermediate, depot-level maintenance, training, or mobile. These summaries help to plan for any modification to an existing facility or development of a new facility.

PHS&T Summaries identify packaging, handling, and storage information.

Post-Production Support Summaries analyze lifecycle support requirements of a system or equipment to ensure supportability over the system or equipment lifecycle.

6.5 NECC Support Concept

Software and hardware to provision a CM will be managed by the cognizant capability provider. The capability provider has the responsibility to establish permanent hosting locations, maintenance agreements, and Help Desk support for the participating CMs. The specific terms of hosting and support requirements are defined for each CM in SLAs between the JPMO and the capability provider. SLAs negotiated will include sustainment requirements and metrics.

The JPMO has responsibility for maintenance of Enterprise-level hardware and infrastructure and procurement of licenses. The CPMOs have responsibility for maintenance of local-site computing infrastructure.

NECC-preventive maintenance is limited to tasks and schedules consistent with mission-performance needs provided in established, planned maintenance systems at each site. NECC-corrective maintenance is performed as required to maintain NECC operational readiness. Contractor Logistics Support (CLS) will be used to satisfy the lifecycle support requirements for all hardware procured by NECC. It is expected that warrantees provided by the original manufacturer will be used to the maximum extent possible.

6.6 Managed Services Strategy

This section describes general requirements for hosted CMs within NECC. The CPMOs delegate implementation of these requirements and document them within the SLAs.

6.6.1 Administration

The responsible CPMO must establish a permanent host location with the following capabilities. This guidance supersedes the applicable SLA.

- 24x7 monitoring and management of the network infrastructure

- Configuration management and access control of network devices
- Information Assurance and Vulnerability Assessment (IAVA) compliance for all network assets
- Real-time monitoring to identify, troubleshoot, and correct network infrastructure issues
- Highly skilled technical support personnel
- Backup and recovery environment
- Disaster recovery resiliency if required by the CM SLA

6.6.2 Storage Solutions

The responsible CPMO must establish a permanent host location with the following capabilities. This guidance supersedes the applicable SLA.

- Backup and archival capability
- Offsite storage depending on requirements
- Encryption of data on the storage media if required

6.6.3 Performance Monitoring

The responsible CPMO must establish a permanent host location with the following capabilities. This guidance supersedes the applicable SLA.

- Performance monitoring for anomaly detection and SLA adherence

6.6.4 Secure Server Builds and Intrusion Detection Systems

The hosting provider ensures the OS and environments are compliant with the local Field Security Office (FSO), to include necessary initial lockdown and maintenance procedures. Systems must meet network connection criteria, which is no Category I findings and no more than 10-15% of Category II and III findings opened.

In addition to local security requirements, the hosting provider must provide Intrusion Detection Systems (IDS) to safeguard NECC data.

6.6.5 Capacity Management

The responsible CPMO must establish a permanent host location with capabilities to meet performance, load, and other criteria mandated by the CM SLA.

6.6.6 Capability Maturity Model Integrated (CMMI) Level of Attainment or Equivalent

If required by the CM SLA, the responsible CPMO must establish a permanent host location that has obtained the required CMMI certification.

6.6.7 Network Availability

NECC provides mission-critical capabilities that will be operational 24/7 in a variety of warfighting environments. These capabilities will support continuity of operations (COOP) by

being distributed across several geographically dispersed nodes. As a result of this distributed architecture, the failure of one or more nodes will not disrupt the overall capability. During such a failure condition, Warfighters will be automatically and transparently redirected to a functioning node hosting the capabilities that they need. The NECC architecture is therefore robust, contains built-in redundancy, and does not have a single point-of-failure. NECC availability will take into account the Planning and NR-KPPs, as prescribed in the CDD.

In addition to supporting Continuity of Operations (COOP), NECC will also provide capabilities tailored to warfighting environments with DIL. NECC will support Service DIL environments, such as ships and forward-deployed command posts. In these environments, it will provide capabilities to Warfighters by means of specially designed data caching and proxy architectures, so that if network connectivity is lost, they will continue to function at the local-level. Then, once connectivity is restored, the NECC capabilities residing at the local level will automatically synchronize with the GIG. Furthermore, NECC will notify Warfighters when connectivity is lost and that they are operating in a local-only mode.

6.6.8 Connectivity

The responsible CPMO must establish a permanent host location with capabilities to meet network connectivity and bandwidth criteria mandated by the CM SLA.

6.6.9 Network Access and Security

The responsible CPMO must establish a permanent host location with the following capabilities. This guidance supersedes the applicable SLA.

- Auditing
- Security Technical Information Guidelines (STIG) compliance
- Physical security

6.6.10 Scalability

The responsible CPMO must establish a permanent host location with the following capabilities. This guidance supersedes the applicable SLA.

- Performance and capacity monitoring
- Scalable hardware and network to meet growth levels defined by the CM SLA

6.6.11 Disaster Recovery

The responsible CPMO must establish a permanent host location with capabilities to meet disaster recovery criteria mandated by the CM SLA.

6.6.12 Facility Description

The responsible CPMO must establish a permanent host location that complies with DISA facility standards for computing facilities. These standards include the height of a raised floor, A/C power, Heating, Ventilation, Air Conditioning (HVAC), fire detection, under-floor water detection, etc.

7 TEST AND EVALUATION

7.1 Test and Evaluation Strategy

The Army Test and Evaluation Command (ATEC) is the lead OTA for NECC. ATEC is supported by the other services' OTAs and the JITC.

The Test and Evaluation (T&E) Strategy supports the NECC objective of continuous capability provisioning by integrating the development, test, and evaluation of many smaller, less complex, loosely connected network services via a virtual environment termed the FDCE. The FDCE increases the interactions and collaborations among the materiel providers, certifiers, Warfighters, and doctrine and requirements communities. Currently, these communities work together to develop and deliver C2 capabilities. However, their current interactions are not as frequent or integrated as necessary to support ongoing NECC CPAs.

The T&E strategy develops FDCE processes and infrastructure in order to mature independent CMs in an evolutionary manner. The FDCE process for maturing CMs divides CPAs into three stages – Development, Developmental Piloting, and Operational Piloting. Each stage represents an increasing level of maturity defined by an increasingly rigorous set of criteria. After meeting the requirements for each stage, the CM obtains a certification that satisfies the entrance criteria for the next stage. The FDCE infrastructure (also known as the "sandbox") implements a set of materiel provider and certifier hardware and software physically distributed on the GIG.

8 SUPPORTABILITY AND PERFORMANCE REQUIREMENTS

8.1 KPPs

The KPPs represent the critical performance parameters that demonstrate the enhanced value of NECC services and provide an objective measure of immediate return-on-investment derived from the initial operational capability of Increment 1.

The NECC KPPs are (1) Shared Situational Awareness, (2) Planning, (3) Training Support to the Warfighter, and (4) Net-Ready Key Performance. The success of NECC is determined by the ability to sustain the capabilities satisfying these KPPs.

8.2 Measures of Effectiveness and Suitability

The Measures of Effectiveness (MOE) and Measures of Suitability (MOS), along with their associated performance requirements, reside in the Test, Evaluation, and Certification (TEC) Criteria Matrix, located in Appendix E of the NECC Test and Evaluation Master Plan (TEMP)[27]. All requirements are traceable to the NECC CDD requirements. The Capabilities Definition Package (CDP) refines the C2 capability requirements found in the CDD or expands upon the C2 capabilities found in the GCCS Requirements Database (GRiD). Compliance with the matrix requirements can be tailorable, depending upon the specifics of the tested CM. MOE and MOS needs are refined based upon a consensus from the T&E Working-level Integrated Product Team (WIPT) members.

[27] DRAFT NECC TEMP, v0.6.0, 25 June 2007, Appendix E, p. 68, https://gesportal.DoD.mil/sites/necc/milestone_launch/default.aspx.

9 NECC Acquisition Strategy

NECC Acquisition Strategy is an evolutionary acquisition strategy, which includes a spiral development approach within distinct increments. Capability will be spiraled out in small bundles on a continuous basis, to cumulatively fulfill the requirements of the defined increment. Each increment is well-bounded and targets specific user requirements and KPPs, as documented in the NECC CDD. For further information, refer to the Acquisition Strategy.

9.1 Acquisition Approach

NECC, as a designated acquisition streamlining pilot program, is authorized to implement streamlining measures, which includes the tailoring of acquisition phases and decision points. Key to this tailored acquisition approach is the NECC program's unique development, test, and certification environment that migrates from a centralized, sequential testing and certification process to a newly distributed, highly parallel approach. This approach allows integration of the assessment, testing, and evaluation procedures to satisfy both the OTA/JITC certification missions and the United States Joint Forces Command (USJFCOM) Joint-interoperable C2 capability mission.

10 Cost Estimates and Funding

For cost estimates and funding, ctrl-click **here**[28].

11 Technology Refresh

Technology refresh is implemented for hardware, software, logistics processes, and training systems and procedures, using upgrade strategies appropriate to the required level of NECC architecture elements.

12 Business Process Improvement

The Business Process Improvement Plan implements an event-driven, rather than a calendar-driven, process.

13 Demilitarization and Disposal

The demilitarization and disposal process requires identifying equipment for disposal that has handled classified information. The amount of equipment that requires disposal is dependent on the level of classification and the service provider implementation. Disposal of this equipment may incur an additional cost to the Government if not negotiated ahead of time with the service provider.

14 Supportability and Risk

The Risk Management Strategy documents the NECC risk management process. Risk management is integral to the NECC program throughout the acquisition lifecycle phases. It helps to determine the priorities of NECC capabilities and the maturity of technologies that could

[28] DRAFT NECC CARD, https://gesportal.DoD.mil/sites/necc/milestone_launch/default.aspx.

provide the capabilities. The process incorporates the use of demonstrations, pilots, trade-off studies, and Maintenance & Support (M&S) activities to evaluate capabilities and technologies with a focus toward minimizing risks. The SE personnel, as part of their overall technical monitoring and control, perform technical risk analysis and subsequent risk management.

14.1 Risk Management Strategy

DoD risk management involves the major activities of risk identification, risk analysis, risk mitigation planning, risk mitigation plan implementation, and risk tracking. Risk management for NECC incorporates these activities and is based on DoD and industry best practices, tailored to meet the needs of the NECC acquisition process.

15 CONFIGURATION MANAGEMENT

The JPMO Operations and ILS Branch (Ops & ILS) establishes and manages NECC configuration management. In this capacity, the JPMO develops and implements configuration management policies and procedures that span across the Materiel Developer community. Included in this role is the JPMO's authority for establishing the NECC's configuration items, such as CMs. The JPMO is responsible for managing and controlling CMs and their related artifacts as they move through the FDCE stages. CM-related artifacts are accessible via the FDCE.

The CPMOs, in their role as Materiel Developers, are responsible for implementing configuration management policies and procedures that maintain adequate configuration control over CMs and their associated engineering software and hardware artifacts. While the JPMO does not dictate how the CPMOs accomplish their configuration management responsibilities, it will provide a minimum set of guidelines that supports the NECC goals.

The NECC CPMO Materiel Developer organizations include the Components' C2 system commands and agencies, as well as other capability providers. These Materiel Developers participate by developing, maturing, operating, and sustaining enterprise-operated CMs. Configuration management supports these Materiel Developers in maintaining, tracking, and providing status accounting of the configured environments, documents, and other products that are part of the piloting environment. The JPMO Ops & ILS Branch maintains a configuration management repository located at Space & Naval Warfare Systems Command (SPAWAR) System Center (SSC) Charleston that supports the NECC in conducting configuration management across the program.

15.1 ENGINEERING REVIEW BOARD (ERB)

The NECC program Configuration Control Board (CCB) uses an ERB, chaired by the NECC Chief Engineer (CE), to conduct a technical review of certain Change Requests (CR) before determining their disposition.

16 INFORMATION ASSURANCE STRATEGY

The IA implementation approach is a multi-pronged strategy, starting with the development of CMs executed by Materiel Developers and managed by the CPMOs. The basic IA security model for NECC is based on distributed C&A. Implementation of security requirements at the CM-level is the responsibility of the CM developers, with CPMO oversight for security

requirements verification. The CPMOs have Certification Authorities (CA) within their Service/Agency to establish the basis for Type Accreditations for the CMs that they are responsible for developing.

17 RECOMMENDATIONS

Recommendations have been coordinated with GIG Sustainment Logistics (GSL) and are being further coordinated with the Systems Engineering Working Group (SEWG). The GSL stated, "It is imperative that the Systems Engineering Team be intimately involved in this process for the conduct of these analyses…" and [these analyses] "… must occur as the design of the NECC capability evolves.[29]"

1. Recommend SE perform Failure Modes Effects and Criticality Analysis (FMECA) to determine the ability to meet KPPs for system operational availability.

2. Recommend SE perform HSI studies to satisfy requirements for environment, safety, health, human factors engineering, and survivability.

3. Recommend the concept of performance-based logistics be embraced by NECC to ensure that the system and equipment design incorporates all of the logistics requirements of (1) maintenance planning; (2) manpower and personnel; (3) supply support; (4) support and test equipment; (5) packaging, handling, storage, and transportation; (6) technical data; (7) computer resources support; (8) facilities; and (9) training and training support.

4. Reiterate for CPMOs and JPMO management that CLS will, with some exceptions (e.g., Navy afloat nodes), be the primary source of support for all commercial products.

[29] DISA GSL Memorandum, dated, 2 Feb 07, subject: Review of the NECC LSA

APPENDIX A – ACRONYMS

AoR	Area of Responsibility
AR	Army Regulation
ATEC	Army Test and Evaluation Command
C&A	Certification and Accreditation
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CA	Certification Authorities
CARD	Cost Analysis Requirements Document
CCB	Configuration Control Board
CDD	Capability Development Document
CDP	Capabilities Definition Package
CLS	Contractor Logistics Support
CM	Capability Module
CMMI	Capability Maturity Model Integrated
COCOM	Combatant Command
COE	Common Operating Environment
COI	Community of Interest
COOP	Continuity of Operations
COTS	Commercial Off-the-Shelf
CPAS	Capability Provisioning Activities
CPMO	Component Program Management Office
CPT	Capability Transition Period
CPU	Central Processing Unit
CR	Change Request

DAG	Defense Acquisition Guidebook
DECC	Defense Enterprise Computing Center
DIL	Disconnected/Intermittently connected/Limited connectivity
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DM	Data Management
DNC	DISA NetOps Center
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
ERB	Engineering Review Board
ESM	Enterprise Service Management
ESOH	Environment, Safety, and Occupational Health
FDCE	Federated Development and Certification Environment
FDCI	Federated Development and Certification Infrastructure
FMEA	Failure Modes Effects Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FoS	Family of Systems
FSO	Field Security Office
GCCS	Global Command and Control System
GCN	GIG Computing Nodes
GES	GIG Enterprise Services
GIG	Global Information Grid
GISMC	Global Infrastructure Service Management Center
GNSC	Global NetOps Support Center
GOTS	Government Off-the-Shelf
GRiD	GCCS Requirements Database

HSI	Human Systems Integration
HVAC	Heating, Ventilation, Air Conditioning
IA	Information Assurance
IAVA	Information Assurance and Vulnerability Assessment
ILS	Integrated Logistics Support
IP	Internet Protocol
IT	Information Technology
JC2	Joint Command and Control
JFC	Joint Force Commanders
JITC	Joint Test Interoperability Command
JMETC	Joint Test Interoperability Command
JPEO	Joint Program Executive Office
JPMO	Joint Program Management Office
JTA	Joint Technical Architecture
JTF–GNO	Joint Task Force – Global Network Operations
JTIC	Joint Test Interoperability Command
JTOCC	Joint Technical Operations Control Capability
KPP	Key Performance Parameter
LAN	Local Area Network
LCC	Life Cycle Cost
LSA	Logistics Support Analysis
M&S	Maintenance and Support
MAIS	Major Automated Information System
MCP	Mission Capability Package
MOE	Measures of Effectiveness
MOS	Measures of Suitability
NCDS	Net-Centric Data Strategy

NCES	Net-Centric Enterprise Services
NCOW RM	Net-Centric Operations and Warfare Reference Model
NECC	Net-Enabled Command Capability
NGO	Non-governmental Organization
NMCS	National Military Command System
NR-KPP	Net-Ready Key Performance Parameter
O&M	Operations and Maintenance
Ops	Operations
OS	Operating System
OTA	Operational Test Authority
PC	Personal Computer
PHS&T	Packaging, Handling, Storage, and Transportation
PSE	Peculiar Support Equipment
PSS	Product Support Strategy
SA	Situational Awareness
SE	Systems Engineering
SEWG	Systems Engineering Working Group
SLA	Service Level Agreement
SLM	Service Level Management
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOAP	Simple Objective Access Protocol
SPAWAR	Space & Naval Warfare Systems Command
SSC	SPAWAR System Center
STIG	Security Technical Information Guidelines
T&E	Test and Evaluation
TD	Technical Development

TEC	Test, Evaluation, and Certification
TEMP	Test and Evaluation Master Plan
TMDE	Test Measurement and Diagnostic Equipment
TMS	Trouble Management System
TNC	Theater NetOps Center
TOCC	Technical Operations Control Center
USJFCOM	United States Joint Forces Command
WAN	Wide Area Network
WIPT	Working-level Integrated Product Team