

UNCLASSIFIED



**Net-Enabled Command Capability
INCREMENT 1 ACQUISITION
INFORMATION ASSURANCE STRATEGY
(IAS)**

Version 1.0

19 July 2007

Prepared by:

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

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

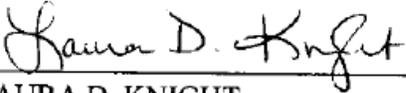
DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (July 2007). Other requests for this document shall be referred to the NECC Program Management Office.

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

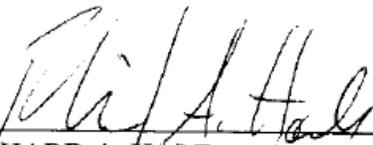
UNCLASSIFIED

UNCLASSIFIED

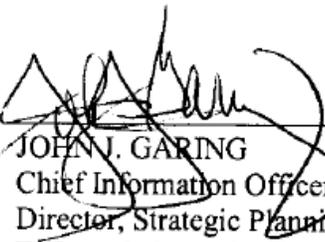
APPROVAL PAGE

Submitted by:  Date: 23 July 2007
LAURA D. KNIGHT
Program Manager,
Joint Program Management Office (JPMO),
Net-Enabled Command Capability (NECC)

Concurred by:  Date: 24 Jul 07
DAVID B. BENNETT
Deputy, Program Executive Office,
Command and Control Capabilities (PEO C2C),
Defense Information Systems Agency (DISA)

Concurred by:  Date: July 25, 2007
RICHARD A. HALE
Chief Information Assurance Executive (CIAE)
Defense Information Systems Agency (DISA)

Concurred by:  Date: July 30, 2007
DIANN L. MCCOY
Component Acquisition Executive (CAE)
Defense Information Systems Agency (DISA)

Approved by:  Date: 8/8/07
JOHN J. GARING
Chief Information Officer (CIO)
Director, Strategic Planning and Information (SPI)
Defense Information Systems Agency (DISA)

UNCLASSIFIED

EXECUTIVE SUMMARY

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD's) principal program for Command and Control Capabilities (C2C) that will be accessible in a net-centric environment and will focus on providing the commander with the data and information needed to make timely, effective, and informed decisions. The Acquisition Information Assurance Strategy (IAS) discusses and summarizes a strategy for identifying Information Assurance (IA) requirements, incorporating them into the Service Oriented Architecture (SOA), identifying threats and risks, conducting security risk management, and achieving and maintaining IA Certification and Accreditation (C&A). Additionally, this document ensures NECC program compliance with the statutory requirements of Subtitle III of Title 40 of the United States Code (40 U.S.C. 11101 et seq.); as directed by DoD Instruction (DoDI) 5000.2.

In the NECC Milestone A Acquisition Decision Memorandum, the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) certified NECC compliance with 40 U.S.C. 11101 et seq.. This certification requires NECC to be managed as "Mission Critical" program as defined in DoDI 5000.2. NECC Capability Modules (CMs) will have a baseline Mission Assurance Category (MAC) of I and a baseline Confidentiality Level (CL) of "Classified".

NECC will use the DoD Information Assurance Certification and Accreditation Process (DIACAP) as the primary C&A vehicle in Increment 1 with the United States Strategic Command (USSTRATCOM) Deputy Commander as the Designated Accrediting Authority (DAA). However, any NECC CMs requiring deployment on Sensitive Compartmented Information (SCI) networks will be accredited using the DoD Intelligence Information Systems (DoDIIS) C&A vehicle and have Defense Intelligence Agency (DIA) as the DAA.

NECC Increment 1 Architecture has been designed in a modular fashion by packaging capabilities, as described in the operational requirements, into CMs, which represent a package of functionally related hardware and software that provides a solution to one or more required capabilities. NECC IA functions will be integrated into NECC CMs as they are defined and developed. The Component Program Management Offices (CPMOs) will integrate these functions consistent with the NECC increment architecture and as specified in the Work Packages (WP) produced by the NECC Systems Engineering (SE) process. Work Packages will designate the IA functional requirements and the IA C&A vehicle(s) to be used. Consistent with "Adopt-before-Buy, Buy-before-Create" ("ABC") acquisition philosophy, key IA components will be adopted and integrated unless during the System Engineering process the JPMO decides to do development.

NECC will use the Information Operations Capstone Threat Assessment (IO CTA), dated January 2006 as the threat baseline. Risk management for NECC is based on DoD and industry best practices, tailored to meet the needs of the NECC acquisition process and implemented through the NECC Risk Management Plan (RMP).

An effective Test and Evaluation (T&E) program will verify and validate the IA requirements of NECC CMs. The Test and Evaluation Master Plan (TEMP) will incorporate IA test requirements. The Joint System Team (JST) is responsible for developing and coordinating the

UNCLASSIFIED

integrated Test and Evaluation (T&E) program. The Federated Development and Certification Environment (FDCE) will provide the environment to support development, integration, testing, and certification of CMs.

The NECC program has several IA dependencies. These include Public Key Infrastructure (PKI) support and certificate management, the acceptance of the NECC Accreditation across DAAs, the leveraging of Net-Centric Enterprise Services (NCES) Security Services, and the adoption of Cross-Domain Solutions (CDS). NECC has a robust approach for managing each of these dependencies. Additional dependencies may be defined as the NECC program matures.

The NECC Acquisition IAS reflects a comprehensive approach to ensuring IA requirements are identified, incorporated, and tested. Additionally, it explains the adoption of threat and risk assessments, the management of risks, and the NECC program's IA dependencies. The delivery of operational capabilities to the Warfighter will be expedited as the NECC program matures and applicable lessons are applied to this document.

UNCLASSIFIED

REVISION HISTORY

REVISION NUMBER	REVIEWER / ORG	CHANGES	REVISION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
0.0.8	DLB/SPEC	Edited document, inserted new title page, created new acronym list, inserted Approval page from Program Control, and defined in text acronyms	17 May 2007	17 May 07	Dustan Brown
0.0.8	NECC Documentation Support	Document reformatting and grammar edits; redefined the setting of the graphics and tables; corrected figure and table referencing; generated a new TOC.	18 May 2007	18 May 07	Issa Jones
0.1.0		Added line numbering; changed the version number to v0.1.0.	18 May 2007	18 May 07	Issa Jones
0.2.0	NECC Documentation Support	Document reformatting	14 Jun 2007	14 Jun 07	Issa Jones
0.2.1	RBG/NECC Documentation Support	Grammar edits	14 June 2007	14 June 07	Becky Gardner
	DLB/SPEC	Reviewed and added edits.	17 June 2007	17 June 07	Dustan Brown
0.2.2	DLB/SPEC	Formatting/Updated program schedule	18 June 2007	18 June 07	Dustan Brown/Doris Cardinale
0.3.0	NECC Systems Engineering	Incorporated comments from formal coordination	3 July 2007	3 July 2007	Steve Brown
0.3.0	DLB/SPEC	Edited and formatted	5 July 2007	5 July 2007	Dustan Brown
0.3.1	NECC Systems Engineering	Incorporated comments from Sr. level formal coordination	18 July 2007	18 July 2007	E. S. Koehler
1.0	BIT (NECC Documentation Support)	Final edit and reformatting	19 July 2007	19 July 2007	Issa Jones

TABLE OF CONTENTS

APPROVAL PAGE.....II

EXECUTIVE SUMMARY III

REVISION HISTORY V

1 INTRODUCTION.....1

 1.1 DOCUMENT SCOPE 1

 1.2 NECC ACQUISITION PHILOSOPHY (‘ABC’ CONCEPT) 2

2 PROGRAM CATEGORY AND LIFE-CYCLE STATUS.....2

3 MISSION ASSURANCE CATEGORY AND CONFIDENTIALITY LEVEL3

4 SYSTEM DESCRIPTION.....4

 4.1 CAPABILITY MODULES AS BUILDING BLOCKS 4

 4.2 PROVIDING CAPABILITIES AS SERVICES 6

 4.3 LEVERAGING EXISTING SYSTEMS 6

 4.4 DEPLOYING CAPABILITIES ON NECC NODES..... 7

5 THREAT ASSESSMENT8

6 RISK ASSESSMENT AND MANAGEMENT.....8

7 INFORMATION ASSURANCE REQUIREMENTS10

8 IA ACQUISITION STRATEGY11

 8.1 SYSTEMS ENGINEERING OVERVIEW 12

 8.2 WORK PACKAGES 12

 8.3 BUSINESS STRATEGY/CONTRACTING 13

 8.4 CERTIFICATION AND ACCREDITATION..... 13

 8.5 NECC FIELDING 15

9 DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP).....16

10 IA TESTING17

11 IA SHORTFALLS AND INCREMENT ONE DEPENDENCIES18

 11.1 PKI SUPPORT AND CERTIFICATE MANAGEMENT..... 18

 11.2 ACCREDITATION ACROSS DAAS 18

 11.3 NCES SECURITY SERVICES 19

 11.4 CROSS DOMAIN SOLUTIONS 20

12 POLICY/DIRECTIVES20

13 RELEVANT ASSOCIATED PROGRAM DOCUMENTS21

14 POINTS OF CONTACT22

APPENDIX A – GLOSSARY.....23

APPENDIX B - ACRONYM LIST25

LIST OF FIGURES

Figure 1: NECC Program Schedule (Top Level)..... 3
Figure 2: NECC Increment 1 Context Diagram..... 7
Figure 3: NECC Capstone Accreditation..... 14

LIST OF TABLES

Table 1: NECC Increment 1 NECC CMs 4
Table 2: Sources of NECC IA Technologies..... 12
Table 3: NECC CM Notional C&A Tasks..... 14
Table 4: Key NECC Certification and Accreditation Roles 16

1 INTRODUCTION

The Net-Enabled Command Capability (NECC) is the Department of Defense's (DoD's) principal program for Command and Control Capabilities (C2C) that will be accessible in a net-centric environment and will focus on providing the commander with the data and information needed to make timely, effective, and informed decisions. NECC draws from the Command and Control (C2) community to evolve current and provide new C2 capabilities into a fully integrated, interoperable, collaborative Joint solution. Warfighters can rapidly adapt to changing mission needs by defining and tailoring their information environment and drawing on capabilities that enable the efficient, timely, and effective command of forces and control of engagements.¹

The NECC program will respond to the Warfighter's needs through disciplined development, test, and user engagement processes. NECC will provide capabilities which focus on Force Projection, Force Readiness, Situational Awareness, Intelligence, Force Employment (Air/Space Operations, Land Operations, Maritime/Littoral Operations), and Force Protection. Its single, net-centric, services-based, C2 architecture will provide the decision support infrastructure that enables the Warfighter to access, display, and understand the information necessary to make efficient, timely, and effective decisions. NECC will leverage existing and evolving C2 capabilities and centers of excellence with its "ABC" commitment to "Adopt-before-Buy, Buy-before-Create." It will deliver continuous C2 enhancements to the Warfighter that evolve NECC towards increased net-centricity and Joint mission integration.

The Acquisition Information Assurance Strategy (IAS) discusses and summarizes the strategy for identifying Information Assurance (IA) requirements, incorporating them into the service architecture, identifying threats and risks, conducting security risk management, and achieving and maintaining IA Certification and Accreditation (C&A).

This Acquisition IAS helps the NECC program office organize and coordinate its Increment 1 approach to identifying and satisfying IA requirements consistent with DoD policies, standards, and architectures. Additionally, this document ensures NECC program compliance with the statutory requirements of Subtitle III of Title 40 the United States Code (U.S.C.), as directed by DoD Instruction (DoDI) 5000.2. As stated in Table E4.1.1 of DoDI 5000.2, the IAS provides documentation that "The program has an acquisition information assurance strategy that is consistent with DoD policies, standards, and architectures, to include relevant standards."

1.1 Document Scope

The Acquisition IAS is a stand-alone living document. Although other key documents referenced within the Acquisition IAS identify supplemental or supporting information, the Acquisition IAS contains sufficient content to communicate clearly the level to which IA is embedded in the NECC acquisition life cycle. Configuration control of the Acquisition IAS will

¹ NECC Acquisition Strategy, Executive Summary, 21 Mar 2007, v0.0.6

be maintained in accordance with the NECC Configuration Management Plan. This NECC Acquisition IAS satisfies the requirements in DoDI 5000.2, DoDI 8580.1, and the Defense Acquisition Guidebook for an Acquisition IAS document.

1.2 NECC Acquisition Philosophy ('ABC' Concept)²

In fulfilling operational requirements outlined by the Joint Combat Capability Developer (JCCD) process, the NECC Acquisition Strategy (AS) embraces the ABC concept: Adopt-before-Buy, Buy-before-Create. In applying the ABC concept to CMs, the program first determines whether a capability in the current Global Command and Control System (GCCS) Family of Systems (FoS) or other C2 systems can be, and should be, adopted to satisfy the requirement, consistent with the NECC SOA. The program expects to transition significant capability from the existing FoS to NECC. If no C2 capability exists that can be adopted to meet the CM requirement, then the NECC program will attempt to purchase an off-the-shelf technology. If a new CM cannot be adopted or bought, then based on a comprehensive ABC Joint Program Management Office (JPMO) decision, NECC will create the necessary capability to meet the requirement. The ABC concept will also be applied to Service Oriented Architecture (SOA) components and IA components in particular in that NECC plans to adopt the Net-Centric Enterprise Services (NCES) Security Services.

2 PROGRAM CATEGORY AND LIFE-CYCLE STATUS

The NECC program is an Acquisition Category (ACAT) 1D program. NECC entered the Technology Development (TD) phase on 7 March 2006 when the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) issued an Acquisition Decision Memorandum (ADM) approving Milestone (MS) A and renamed the Joint Command and Control (JC2) program as the Net-Enabled Command Capability (NECC) program. The TD phase allows NECC to reduce technology risk and to define and evaluate appropriate processes, which enable the development and delivery of capabilities in a net-centric environment. The TD phase will culminate in a MS B decision that establishes a new acquisition program and enters NECC into the System Development and Demonstration (SDD) phase. The objective date for the NECC MS B decision is September 2007. In the NECC Milestone A ADM, ASD(NII) certified NECC compliance with 40 U.S.C. 11101 et seq. This certification requires NECC to be managed as a "Mission Critical" program as defined in DoDI 5000.2. The DoD Information Technology Portfolio Repository (DITPR) reflects this designation. NECC will be an evolutionary acquisition occurring over multiple increments. It is currently preparing for Increment 1 of its life cycle as depicted in Figure 1.

² Derived from NECC Acquisition Strategy, Paragraph 4, 17 May 2007, v0.2.0

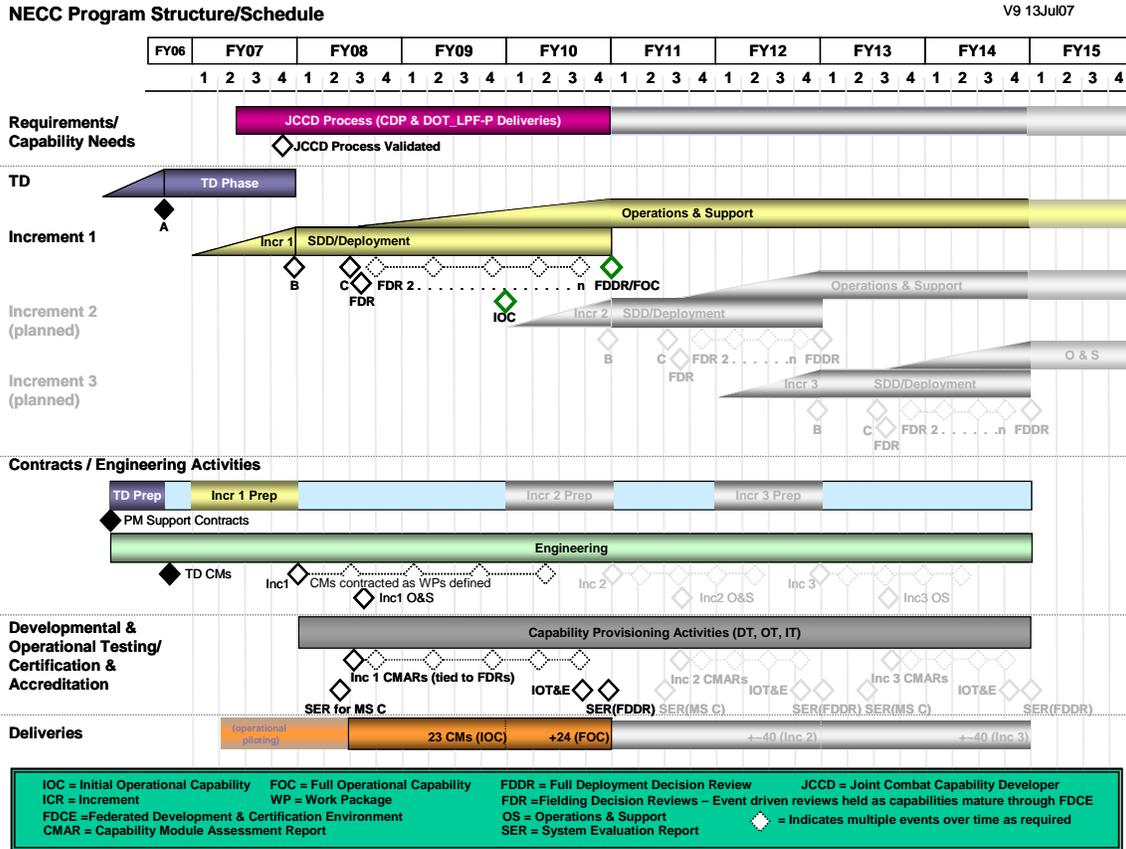


Figure 1: NECC Program Schedule (Top Level)

3 MISSION ASSURANCE CATEGORY AND CONFIDENTIALITY LEVEL

The Mission Assurance Category (MAC) reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the Warfighters' combat mission. The Confidentiality Level (CL) establishes acceptable access factors such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system. MAC and CL are formally defined in DoDI 8500.2, Enclosure 2, Paragraph E2.1.38.

NECC CMs will have a baseline MAC of I and CL of Classified. The MAC and classification baseline reflects the highest levels of IA. For any specific NECC CM, one of two methods may modify this baseline:

1. The MAC and CL may be modified in the NECC Systems Engineering (SE) process during the preparation of CM requirements with the coordination of the NECC Joint Program Executive Office (JPEO) and the JCCD.
2. The JCCD may associate a modified MAC and CL with specific requirements in a Capabilities Definition Package (CDP). NECC products resulting from these requirements

may then be assigned the CDP specified MAC and CL based upon the intended use and deployment environment for that CDP.

NECC will also include CMs that will be deployed in Sensitive Compartmented Information (SCI) and coalition environments. Refer to Section 8.

4 SYSTEM DESCRIPTION³

In order to get capabilities to the Warfighter faster, NECC plans to continuously field solutions as they are developed and tested, instead of the traditional approach of waiting until the end of the SDD phase to test and field the entire solution. To support this continuous-fielding paradigm, the NECC Increment 1 Architecture has been designed in a modular fashion by packaging capabilities, as described in operational requirements, into CMs. Each CM represents a package of functionally related software that provides a solution to one or more required capabilities. An increment-specific architecture effort will produce a set of logical CMs based on the Capability Development Document (CDD) Extension D, “Mission Capability Packages (MCPs) List and Description,” requirements that are used in design and functional development efforts. While there may be dependencies between CMs, the specifications allow them to be built and fielded independently. The modular NECC Increment 1 Architecture will allow NECC to develop and field CMs rapidly throughout the three-year Increment 1 phase and will provide the first set of capabilities to the Warfighter in FY08.

4.1 Capability Modules as Building Blocks

The CM is the primary building block of the NECC architecture. The set of CMs in the NECC architecture has been identified through analysis of the CDD, which spans six functional domains (Adaptive Planning, Force Projection/Force Visibility, Intelligence, Situational Awareness, Force Employment, and Force Protection) and is very conducive to a continuous fielding paradigm. While there are some dependencies across the six functional domains, the materiel solution built to meet the requirements of one domain can be constructed and fielded independently from the other five domains. For example, the *Force Projection* solution can be built and fielded prior to releasing the *Adaptive Planning* solution. Table 1 shows the proposed NECC CMs for Increment 1.

Table 1: NECC Increment 1 NECC CMs

Functional Domain CMs		C2 Cross-functional CMs
1. Adaptive Planning		
Adaptive Planning: Employment Planning		Redirection
Employment Plan Data	Strategic Guidance	Geospatial Rendering

³ Dr. Mark Matthews, Increment 1 Architecture Overview, 9 Apr 2007, v0.2

UNCLASSIFIED

Functional Domain CMs		C2 Cross-functional CMs
Concept Course of Action (COA) and Effect Development	Plan Development and Refinement	Analysis and Reporting
Adaptive Planning: Deployment Management		Orchestration
Deployment Data	Deployment Plan Management	C2 Collaboration
Sustainment Estimation	Transformation Management	User Management
Adaptive Planning: Execution Management		C2 Messaging
Employment Execution	Deployment and Distribution Visibility	
Joint Force Synchronization		
2. Force Projection / Force Visibility		
Force Projection / Force Visibility: Force Structure		
Joint Force Structure Data	Army Force Structure Data	
Navy Force Structure Data	U. S. Air Force (USAF) Force Structure Data	
U. S. Marine Corps (USMC) Force Structure Data	Force Structure Management	
Force Projection / Force Visibility: Capability Visibility		
Force Location and Availability Data	Force Apportionment Data	
Capability Based Force Options		
Force Projection / Force Visibility: Global Force Readiness		
Joint Readiness Data	Army Readiness Data	
Navy Readiness Data	USAF Readiness Data	
Readiness Assessment & Analysis		
3. Intel		
Imagery Data	Collection Management	
4. Situational Awareness		
Red Track Data	Weather Data	
Blue Force Ground Data	Blue Force Maritime Data	
Blue Force Air Data	Global User Defined Operational Picture (UDOP)	
Association Management		
5. Force Employment		
Force Employment: Air/Space Operations		
Air Task Order Data	Air Space Management Data	
Air Mission Planning Data		
Force Employment: Ground Operations		
Army Maneuver Data	Army Fires Data	

Functional Domain CMs		C2 Cross-functional CMs
6. Force Protection		
Missile Defense and Warning		

4.2 Providing Capabilities as Services

NECC is a SOA where each CM provides one or more services accessible via a set of public interfaces. Externally, a CM appears as a collection of services, but internally it may be implemented with Web Services (WS), relational databases, legacy applications, or other software components.

CMs provide services for NECC to publish its authoritative data to the Global Information Grid (GIG). For example, the *Deployment Data CM* in Table 1 publishes authoritative deployment data. CMs also provide services that interact with data CMs to provide a functional capability to the end-user. For example, the *Deployment Plan Management CM* accesses data from the *Deployment Data CM* to provide the end-user with a view of the hierarchical relationships between force modules supporting a deployment operation. Some CMs provide infrastructure services for use by other CMs. For example, the NECC Increment 1 Architecture includes CMs that provide IA (as a part of User Management) and data management services for use by other CMs.

4.3 Leveraging Existing Systems

One of the main drivers of the NECC Increment 1 Architecture is the ABC acquisition strategy that requires NECC to adopt existing solutions before buying or creating new solutions. In keeping with this strategy, the NECC architecture leverages many capabilities provided by other DoD programs. Figure 2 identifies the primary systems that NECC will leverage to meet the CDD requirements.

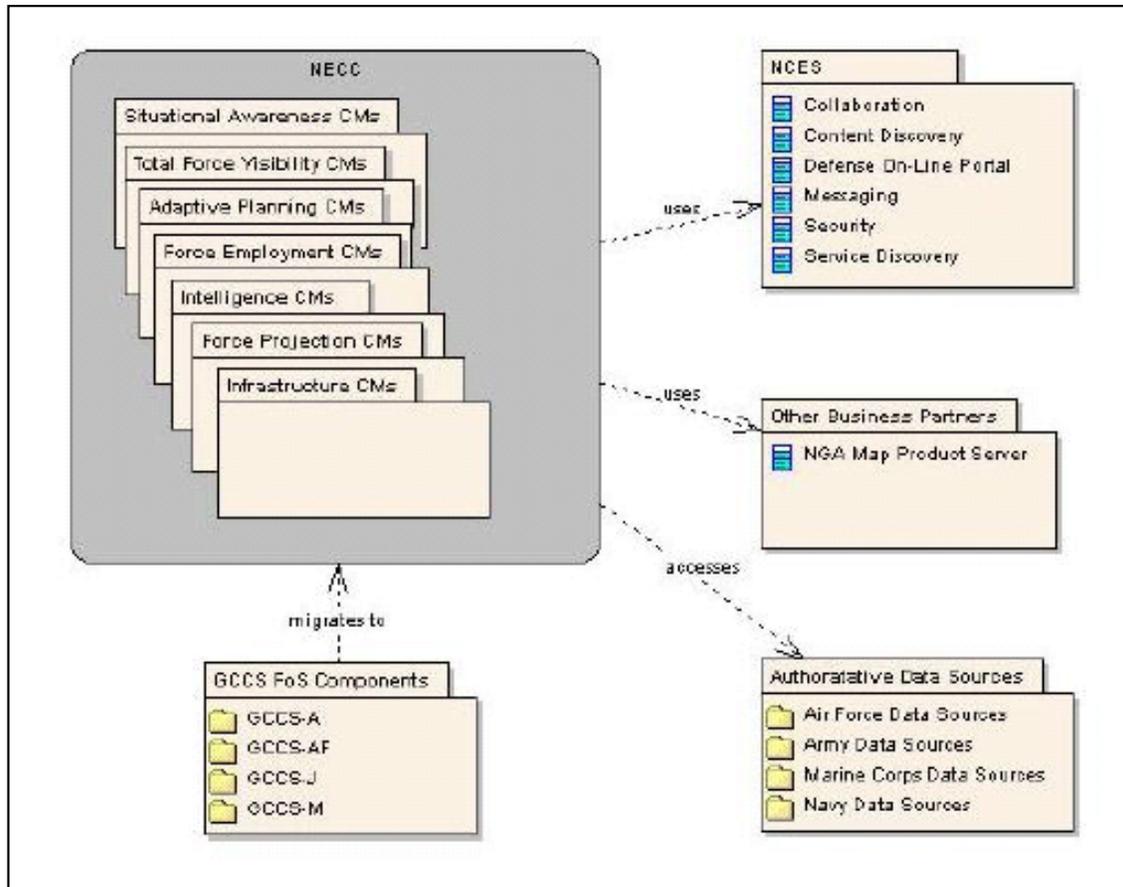


Figure 2: NECC Increment 1 Context Diagram

As depicted in Figure 2, NECC will use services provided by the NCES program and other business partners, such as the *National Geospatial-Intelligence Agency* (NGA). NECC will use NCES collaboration, security, content discovery, service discovery, messaging, and portal services as they become available. Business partnerships will be established with other DoD and/or Federal organizations, such as NGA, to provide NECC capabilities.

The set of authoritative DoD C2 data is distributed across a large number of existing C2 systems. NECC will develop CMs that will provide access to existing and future data sources.

Over time, NECC will replace the *GCSS FoS* allowing these legacy systems to be retired. This migration of *GCSS FoS* functionality into NECC will begin in Increment 1 and will last throughout several NECC increments. In Increment 1, the migration will begin as NECC “adopts” and adapts existing net-centric implementations from the *GCSS FoS*.

4.4 Deploying Capabilities on NECC Nodes

NECC CMs will deploy two types of nodes: Enterprise GIG Computing Nodes (GCNs) and Local GCNs. Enterprise GCNs will provide services to a large number of users connecting to NECC over a wide area network. During Increment 1, the Defense Enterprise Computing Centers (DECCs) or other DECC-equivalent sites will host approximately five enterprise nodes.

The exact location of the enterprise nodes will be determined early in the SDD phase. Local GCNs will provide services to a number of users connecting to NECC over a local area network. Local nodes will be located at sites that have requirements to support Disconnected/Intermittently connected/Limited connectivity (DIL). Local nodes will host the set of CMs needed by the users at the local site. The complexity of the deployment environment will require the development of numerous Service Level Agreements (SLAs) between the NECC program and the organizations hosting NECC capabilities.

5 THREAT ASSESSMENT

NECC will use the Information Operations Capstone Threat Assessment (IO CTA), dated January 2006 as the threat baseline. The IO CTA is the Defense Intelligence Agency (DIA)-validated authoritative source for all threats to DoD information systems and information technology.

The Principal Accrediting Authority (PAA) has indicated that the Designated Accrediting Authority (DAA) will determine the need and nature of an additional threat assessment (Surveillance and Target Acquisition (STA), IO threat assessment or other capstone assessment) to be performed by DIA. The DAA has determined that the IO CTA is sufficient and an additional threat assessment is not required at this time.

6 RISK ASSESSMENT AND MANAGEMENT

DoD risk management involves the major activities of risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking. Risk management for the NECC program is based on DoD and industry best practices, tailored to meet the needs of the NECC acquisition process and implemented through the Risk Management Plan (RMP). The objective of the NECC RMP is to implement a formal, forward-looking, and continuous risk management process that primarily controls risks through risk mitigation planning and implementation rather than solely relying on risk avoidance, transfer, or assumption. This approach is based on the procedures outlined below:

- DoDI 5000.2, Operation of the Defense Acquisition System
- Risk Management Guide for DoD Acquisitions, Sixth Edition; Federal Information Security Management Act (FISMA) of 2002
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems
- DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), the process for managing risk associated with network PPSM
- DoDI O-8530.2, Support to Computer Network Defense (CND)

These procedures establish a requirement for all operational DoD information systems to establish a service relationship with a Computer Network Defense Service Provider (CNDSP). The DoD Information Assurance Certification and Accreditation Process (DIACAP) will ensure that association with a CNDSP is a condition of full certification or a risk consideration in an accreditation decision.

UNCLASSIFIED

The program will monitor and assess risk as part of its RMP execution and ongoing analysis. The NECC Chief Engineer (CE), IA Manager (IAM), NECC Risk Management Coordinator, and DAA will monitor risk and apply mitigations. The JPMO will conduct risk assessments for each increment as part of the required Acquisition IAS process. The DAA determines whether the residual risk of the NECC Increment 1 Architecture, to include CMs, is at an acceptable level or if additional security controls are necessary to reduce or eliminate the existing risk prior to accreditation and throughout the life cycle of the system.

NECC is integrating continuous risk management into the NECC life cycle, which includes security risks. As risk management is an iterative process, assessments will be performed during each major phase of the NECC life cycle: Technology Development, SDD, Production and Deployment, and Operations and Support. Iterative assessments will also be conducted regularly throughout the Capability Provisioning Activities (CPAS) development stages: Development, Developmental Piloting, and Operational Piloting. Risks and associated risk levels are determined by the likelihood of threat exploitation, magnitude of impact, and the adequacy of planned or current controls in accordance with a standard DoD risk management reference, *Risk Management Guide for DoD Acquisition*.

NECC IA risk assessment results are assigned through Impact and Severity codes. The Impact Code indicates DoD's assessment of the likelihood that a failed IA control will have system-wide consequences. Specifically, the impact code describes the impact associated with non-compliance or exploitation of the IA control. In addition, the impact code determines the urgency with which corrective action should be taken. Impact codes are expressed as High, Medium, and Low where High is the indicator of greatest impact or urgency. IA Severity Codes reflect the Certifying Authority's (CA's) assessment of the likelihood of exploitation of a given IA vulnerability. To be clear, severity codes are documented as Category (CAT)-I, CAT-II, and CAT-III. CAT-I indicates the greatest risk and urgency. As a result, the combination of impact and severity codes determine the level of risk associated with non-compliance and provide a metric for the urgency with which corrective action must be taken. In spite of the impact and severity codes, the CA may determine that overall risk of the IA requirement is reduced due to the presence of risk mitigation efforts.

As part of the DIACAP process, each CM will receive a risk assessment. The Federated Development and Certification Environment (FDCE) will provide access to the DIACAP Plan of Action and Milestones (POA&M) which documents the required corrective actions imposed by the DAA to lessen the risk associated with operation of the CM. The POA&M also includes the agreed upon timeline for completing and validating corrective actions, and the resources required. The DIACAP Scorecard, also made accessible through the FDCE, summarizes the implementation status of the assigned IA controls that have been certified or accredited to support or convey a certification determination. After a POA&M is developed, an abstracted high-level version of the risk may be added to the risks identified in the NECC RMP. However, the details of the POA&M will not typically be tracked within the NECC RMP. The Defense Information Systems Agency's (DISA's) Chief Information Officer (CIO) is responsible for monitoring and tracking the overall execution of the POA&M(s) until the identified security weaknesses have been addressed and the C&A documentation updated. DIACAP additionally directs an annual review of IA posture in accordance with FISMA.

7 INFORMATION ASSURANCE REQUIREMENTS

IA requirements document the IA functions and capabilities (technical mechanisms and non-technical controls) that will enable the NECC CMs to ensure the ongoing confidentiality, integrity, and availability of the data handled by those CMs when that data is either in use, in transit, or at rest. CM IA requirements will be tailored according to their assurance levels (MAC and CL under DIACAP) and inherent risks. CM IA requirements will be tracked as the CM progresses from development, developmental piloting, and operational piloting continuing throughout the lifetime of the CM. The CA and DAA will approve the tailoring of the IA requirements and will monitor implementation through the C&A process.

IA requirements for NECC will be managed within the NECC FDCE using the Test, Evaluation, and Certification (TEC) criteria⁴ developed by the NECC Test community, and IA tools such as the IA Compliance Assessment Tool (IA CAT). The TEC criteria are mechanisms that provides discrete, net-ready, IA, interoperability, performance, and mission capability requirements that can be tested individually to evaluate the degree to which a CM is compliant with established test and certification policies, regulations, and validated operational mission requirements.

The NECC CDD is the primary operational requirements document driving the NECC SDD phase. Additionally, the following bulleted list contains other key sources of NECC IA requirements:

- **Assurance Level Controls:** In non-SCI enclaves, NECC CMs will comply with IA controls identified in DoDI 8500.2 based on the CM's MAC and CL. NECC will establish baseline IA controls from DoDI 8500.2 using MAC-I and CL-Classified. The NECC JPMO has begun an assessment of these controls in a preliminary implementation plan. This implementation plan begins the process of determining which controls will need to be provided by NECC software and which controls will be provided through organizations that host NECC software. This early planning should facilitate type accredited NECC software for rapid fielding at numerous host sites. In SCI enclaves, NECC will comply with controls appropriate to the Director of Central Intelligence Directive (DCID) 6/3. MAC, CL, Protection Level (PL), and Level of Concern for Integrity and Availability will be derived from identified user requirements and defined early in the NECC SE process during the development of the CDPs.
- **Governing Policies and Directives:** The policies and directives specified in Section 12, "Policy/Directives" of this document mandate IA functionality and security properties that will be incorporated into NECC. Examples of policy that will be required to be followed include National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, which dictates the use of certified IA products.
- **Findings of Threat and Risk Assessments:** Threat assessments will determine if potential threats to a system exist and the likelihood of that threat actually occurring to the system. By considering both threat and vulnerabilities, risk assessments determine the amount of residual

⁴ TEMP, v0.6.0, 25 June 2007, Appendix E, p. 68

risk of a threat occurring and its potential damage after IA countermeasures have been implemented. A finding of unacceptable residual risks will require further management action by the NECC materiel provider (the NECC materiel provider is the government entity, usually a Component Program Management Office (CPMO), responsible to the JPMO for the delivery specified NECC capability).

- **Standards-Driven Requirements:** Given the inherent risks posed by the technologies NECC will leverage, NECC acquisition and development will require the secure use of security technical standards (e.g., WS-Security and Security Assertion Markup Language (SAML) with Simple Object Access Protocol (SOAP); Extensible Markup Language (XML) Digital Signature and XML Encryption; WS-Secure Conversation and WS-Trust; and Transport Layer Security (TLS)). NECC will comply with IA standards specified in the DoD Information Technology Standards Registry (DISR) online.
- **Stakeholder Requirements:** Beyond those derived from the other sources, any additional security requirements specified by NECC stakeholders will be captured through their ongoing participation in the IA Working-level Integrated Product Team (WIPT) and will be identified in CDPs developed by USFCOM. Additional requirements may also stem from interaction with other programs of record to ensure NECC satisfies their IA requirements.
- **Security Technical Implementation Guides:** NECC CMs will be developed in accordance with all applicable Security Technical Implementation Guides (STIGs) published by the DISA Field Security Operations (FSO), and are intended to be operated in STIG compliant environments. In the absence of a DISA STIG, developers should use appropriate National Security Agency (NSA) configurations guides, if available.
- **Training and Certification:** In accordance with DoD Directive (DoDD) 8570.1-M, the NECC IA workforce will meet IA training and certification requirements and provide required, recurring IA and security training for all program personnel.

NECC will plan for costs associated with these IA requirements. IA development, test, implementation, and maintenance costs (including costs associated with C&A activities) will be included in the overall budget formulation for each CM and documented in the CM Work Packages (WPs). These costs will be programmed through the Program Objective Memorandum (POM) cycle. Technical, schedule, cost, and funding issues associated with satisfying IA requirements will be projected for each CM. Detailed information on CM IA costs will be identified and tracked in the CM Spend Plans and other budget planning tools.

8 IA ACQUISITION STRATEGY

IA will be integrated into NECC CMs as they are defined and developed. NECC IA capabilities will be incorporated into NECC CMs by the CPMOs consistent with the NECC Increment 1 Architecture and as specified through the NECC SE process. IA components will be adopted and integrated rather than developed, whenever possible; some examples are provided in Table 2.

Table 2: Sources of NECC IA Technologies

Sources	Supported IA Functions
DoD Public Key Infrastructure (PKI)	Authentication, Non-repudiation, Data Integrity
NCES Security Services	Authorization
DoD Guard Technologies (e.g., Radiant Mercury, Information Support Server Environment Guard, DataSync Guard)	Cross-Domain Solutions (CDS)

Below is a description of the NECC engineering and acquisition process that includes IA acquisition.

8.1 Systems Engineering Overview⁵

The NECC CDD lays out the C2 needs for the Warfighter. Over the course of the program, requirements developers use the JCCD process to generate CDPs. NECC engineers perform standard systems engineering on these CDPs to produce, over time, a baseline set of CMs. The program then allocates CM development to the CPMOs via WPs. The first WP describes the development, integration, test, and certification requirements for the CM. The second WP describes implementation, which includes fielding, monitoring, and sustainment. All WPs address cost, schedule, IA, and performance requirements; shared resource coordination; and other agreements and dependencies required to produce and sustain the CM. The NECC program merges WPs for multiple capabilities where appropriate to reduce redundant efforts.

8.2 Work Packages⁶

NECC’s development process defines WPs over time. All WPs are not defined prior to MS B, but are developed over the course of the program’s SDD phase. This ongoing system engineering analysis of WPs differs from a typical software development program and affects the program’s decision reviews. These reviews are not focused on the CMs themselves, but rather the processes used to develop the CMs. For each CM, WPs will designate the IA policy vehicle(s) to be used (DIACAP or DoD Intelligence Information Systems (DoDIIS)) and baseline IA requirements (MAC/CL or PL). WPs that include IA services will contain the requirement for personnel training and certification of IA in accordance with DoDD8570.1. These requirements will flow down to contractors as required. WPs will also include a requirement that all Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf

⁵ NECC Acquisition Strategy, Executive Summary, 19 Apr 2007, v0.1.0

⁶ NECC Acquisition Strategy, Executive Summary, 19 Apr 2007, v0.1.0

(GOTS) IA products, and IA enabled products employed by NECC must comply with NSTISSP No. 11.

8.3 Business Strategy/Contracting⁷

The overarching NECC contracting approach is to acquire CMs, services, and materiel from various types of full and open, competitively awarded performance-based and performance-driven outcome contracts. NECC's primary contracting method uses Indefinite Delivery/Indefinite Quantity (IDIQ) contracts to develop CMs. The NECC JPMO and CPMOs, acting as NECC systems integrators/materiel providers, have the flexibility to award multiple Task Orders (TOs) under these vehicles. The intent is to leverage various types of existing and logical follow-on contracts associated with GCCS FoS programs. In many cases, NECC TOs are competed among the numerous vendors available under these IDIQ contracts through the fair opportunity to compete process required by the Federal Acquisition Streamlining Act (FASA). In instances in which using an existing IDIQ contract is not feasible, NECC acquires services and materiel through a full and open competitively awarded contract. NECC uses Federally Funded Research and Development Centers (FFRDC), Systems Engineering and Technical Assistance (SETA), and small business procurement opportunities. NECC accesses some services and materiel through Military Interdepartmental Purchase Requests (MIPRs) to a fee-for-service Government Agency/Service. NECC will comply with the Economy Act and proper use of non-DoD contract requirements.

8.4 Certification and Accreditation⁸

United States Strategic Command (USSTRATCOM) has been appointed as NECC's DAA for accreditation of non-SCI CMs. Meanwhile, FSO has been proposed as the Certification Authority (CA). The overall DIACAP accreditation has been determined as MAC I, Classified.

The program seeks "type accreditation" approval for NECC CMs. Once the CM is accredited for the GIG, it may be rapidly deployed to NECC enterprise nodes and local nodes, to meet user requirements.

NECC will use the DIACAP as the primary C&A vehicle in Increment 1 with the USSTRATCOM Deputy Commander as the DAA. The NECC SE process will derive any requirement for fielding on SCI networks from the operational requirements in the JCCD produced CDPs. Any NECC CM requiring deployment on SCI networks will be accredited using the DoDIIS C&A vehicle.

DIA has been appointed as NECC's DAA for certification of SCI CMs. As the technical requirements have not been defined, the overall DCID 6/3 accreditation has not yet been determined.

⁷ NECC Acquisition Strategy, Paragraph 7.2, 17 May 2007, v0.2.0

⁸ NECC Acquisition Strategy, Executive Summary, 19 Apr 2007, v0.1.0

The NECC architecture will be included and accredited under the NECC Capstone Accreditation Package. Within the NECC Capstone Accreditation, CMs will be grouped by C&A policy vehicle. Accreditation decisions made by both DAAs will be independently documented, but managed as a single capstone accreditation. Figure 3 depicts the NECC Capstone Accreditation.

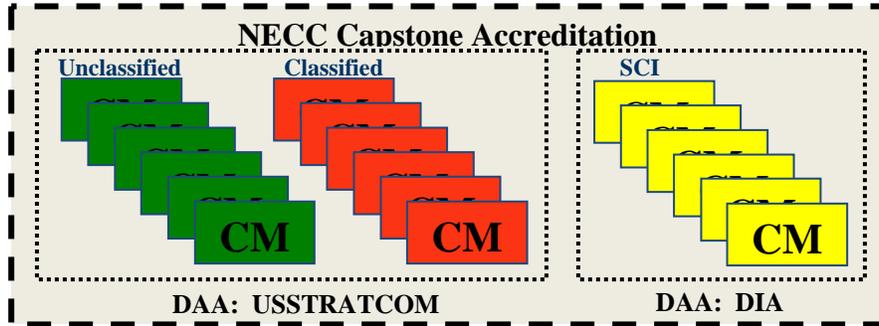


Figure 3: NECC Capstone Accreditation

As NECC anticipates an eventual, long-term need for CMs supporting non-DoD federal systems (e.g., Department of Homeland Security (DHS)), NECC will also include CMs C&A using the National Information Assurance Certification and Accreditation Process (NIACAP) per the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000 under the NECC Capstone Accreditation once this requirement is deemed necessary. A DAA has not been appointed for NIACAP CMs at this time. NECC maintains a cross-matrix of IA requirements for each C&A policy vehicle to document the translation of implemented IA requirements for each CM.

As a CM transitions through the development stages and reaches the level of maturity in which the CM is deemed ready for operational use, the CA makes a certification recommendation to the DAA. The DAA reviews the certification artifacts and makes a determination whether the CM meets the minimum security requirements and, consequently, is included in the NECC Capstone Accreditation. The NECC Capstone Accreditation, required for MS C, will include only those CMs that have been certified during post MS B and prior to MS C by the NECC DAA. The specific details on how CMs will be evaluated will be documented in the NECC C&A process. Table 3 lists a notional set of C&A tasks. These notional tasks are then tailored based upon the maturity of a specific CM.

Table 3: NECC CM Notional C&A Tasks

NECC CM NOTIONAL C&A TASKS
Initiate and Plan IA C&A
Review CM Work Package
Consider the C&A approach (i.e. DIACAP, DCID, NIACAP)
IA Registration (System Identification Profile (SIP))
Identification of Capability Module Test Team (CMTT) Resources
Post All Existing C&A Documentation (if applicable)
Tailor IA Requirements Matrix (Profile)

UNCLASSIFIED

NECC CM NOTIONAL C&A TASKS
Formalize the Accreditation Boundary
Identify External Connections and Connection Rules
Develop Security Input to the SLA
Create Initial Draft of Capability Security Plan (CSP)
Develop IA Implementation Plan
Perform Program Risk Assessment
Implement and Validate Assigned IA Controls
Develop CM Using DISA STIGs, NSA System Network Attack Centers (SNACs), etc
Update and Complete CSP
Joint System Team (JST) Develops Test Plan
Test Tool Identification
CMTT Develops Test Cases
Materiel Provider Performs Self-Certification
CMTT Asserts Certification Tests Are Valid
IA POA&M
Make Certification Determination & Accreditation Decision
Complete DIACAP Scorecard
CA Makes Certification Determination
Produce Summary Briefing for DAA
DAA Makes Accreditation Decision or Appends to Existing Accreditation
Maintain Authority to Operate and Conduct Reviews
Maintain Situational Awareness (Annual IA Controls Review)
Maintain IA Posture (Revalidate IA Controls As Needed)
Decommission
Retire System Decision
Retire System

8.5 NECC Fielding⁹

The JPMO fields all Increment 1 capabilities at the DoD Enterprise level. The collection of Enterprise GCNs provides Quality of Service (QoS) and Continuity of Operations (COOP) for NECC users worldwide with good connection to the GIG. As new CMs are certified and accredited for operational use, they are made immediately available at all existing enterprise

⁹ NECC Acquisition Strategy, Executive Summary, 19 Apr 2007, v0.1.0

nodes. Selected NECC CMs are hosted locally at designated Service/Component commands and units in order to provide critical C2 capabilities when these commands/units are disconnected from the GIG. The sites that contain these Local GCNs and the list of critical CMs to be hosted at each of these sites are determined by the responsible Service/Component CPMOs based on the warfighting mission needs and COOP requirements of the sites. NECC CMs are "type" accredited by the NECC DAA, and must be incorporated into the host site's accreditation as described in the NECC C&A process document. NECC CMs are designed to "inherit" compliance for select IA controls from the host site. Therefore, it is essential the host site verify the adequacy of inherited controls to ensure NECC CMs can be operated at an acceptable level of risk consistent with the "type" accreditation.

9 DoD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP)

NECC will use the DIACAP as the primary C&A vehicle in Increment 1. Any NECC CMs requiring deployment on SCI networks will be accredited using DCID 6/3 C&A vehicle under DoDIIS and have DIA as the DAA. NECC CMs requiring deployment on both SCI and non-SCI networks will require accreditation under both DIACAP and DoDIIS. The IA guidance governing the implementation of IA in the SCI environments and CDS will be considered in the Increment 1 IA implementation to ensure that long range strategies are not jeopardized by the short-term emphasis on the collateral network and DIACAP.

The following offices and individuals are responsible for the successful C&A of NECC CMs. The USSTRATCOM Deputy Commander is appointed as the NECC DAA. The DISA FSO is the CA. In accordance with DoDD 8570.1-M, the NECC Joint Program Manager (JPM) will designate an IAM. The NECC IAM will orchestrate the overall C&A process and ensure IA diligence in supporting approval for the NECC baseline product and all major or minor upgrades. The DAA, CA, IA Validators, and NECC IAM will ensure IA controls are maintained when the NECC Configuration Control Board (CCB) approves service upgrades, patch updates, and new releases. Table 4 identifies roles of the parties involved in C&A of NECC capabilities. The C&A Strategy will be reviewed and approved at all working levels to include the CA and DAA representative.

Table 4: Key NECC Certification and Accreditation Roles

Title	Organization	Role
Director for Command, Control, Communications, and Computer Systems	Joint Staff	Warfighting Mission Area PAA
Deputy Commander	Headquarters U.S. Strategic Command	NECC DAA (DIACAP)
Chief Information Assurance Officer	Defense Intelligence Agency	NECC DAA (DoDIIS)
Field Security Office	Defense Information Systems Agency	CA
Joint Program Manager	NECC Joint Program Office	NECC PM
IA Manager	NECC Joint Program Office	NECC IAM
Director, Requirements and Integration	Headquarters U.S. Joint Forces Command (USJFCOM)	NECC User Representative

The NECC JPM, IAM, and CCB will approve the product version upgrades, patch updates, and subsequent releases ensuring integration compatibility and IA compliance. The NECC DAAs, NECC CA, and NECC IA Team will ensure IA diligence in approving NECC baseline product version upgrades, patch updates, and major releases. The JST is an additional agent responsible for exercising IA diligence for major releases.

DISA, the component services, and the Combatant Commands (COCOMs) will be involved in using the FDCE for CM development, integration, testing, and certification. The FDCE has defined a set of processes to be used in supporting certification (including functional, infrastructure, and security) of CMs at various levels of maturity. In addition, the FDCE will provide infrastructure components that will have been certified and accredited to support development, developmental piloting, and operational piloting. The FDCE will incorporate links to tools, which facilitate DIACAP. The FDCE will support IA testing. In particular, it will be used to capture new and existing IA test artifacts.

10 IA TESTING

IA testing not only provides the data to determine compliance with security requirements; it is also the primary method of ensuring IA diligence throughout the engineering cycle.

IA test requirements will be incorporated into the NECC TEMP. An effective Test and Evaluation (T&E) strategy will be developed for verifying and validating NECC IA requirements.

JST is responsible for developing and coordinating the integrated T&E program and for providing a focal point for NECC T&E issues in support of Warfighter requirements. The JST will facilitate the development and management of the NECC test strategy, TEMP, a System Evaluation Plan for each NECC CDP, Operational Test Agency (OTA) test plans for system test events, and T&E reports through Full Operational Capability (FOC). The JST is directed to ensure the development of both the NECC T&E strategy and to provide guidance regarding format, organization, content, submittal, coordination, approval, and updates.

The JST will establish an integrated test team (CMTT) to test specific CMs from development through fielding. The NECC JPMO will designate a Developmental Test (DT) lead and the lead OTA will designate an Operational Test (OT) lead for each assigned CMTT. The overall CMTT lead is defined by the test event and the responsibility will transfer based upon the test event being planned and executed. The CMTT will be responsible for performing a Risk Assessment on assigned CMs to determine the level of testing required. CMTTs will perform all test planning activities including planning meetings and working groups. CMTT will execute CM level testing, conduct data analysis, and provide CM Assessment Reports (CMARs). An IA Validator will be assigned on a CM-by-CM basis and will participate on each CMTT.

The NECC JPMO will provide an Information Systems Security Engineer (ISSE) to participate in the JST as the DAA's IA advocate. The ISSE lends security expertise and provides knowledge and guidance to the JST and CMTT members where IA testing matters are concerned.

IA test execution begins after the materiel provider asserts that the IA requirements have been met with specified controls and conducting self-certification testing. The IA Validator,

appointed to the CMTT, reviews the certification artifacts and validates whether the implemented controls meet the intent of the requirement. The CMTT may conduct additional certification testing to assess the level of risk, if desired. The JST confirms that the requirements have been validated. The JST Charter document contains additional information about the JST and CMTT.

11 IA SHORTFALLS AND INCREMENT ONE DEPENDENCIES

Based upon the current NECC budget plan for Increment 1, no significant IA funding shortfalls have been identified at this point; however, several engineering dependencies have been identified and are included below. These dependencies may result in reduced NECC function or delivery schedule slippage if problems are encountered in the future.

11.1 PKI Support and Certificate Management

PKI, which is a critical support infrastructure for the GIG, is used to issue credentials to human users, as well as non-human entities (e.g., WS providers, applications, processes, computing devices, and other network elements). Since portals can be configured to trust certificates issued by multiple CAs, users can access authorized portals across the different network domains supported by those CAs. The current DoD PKI supports the issuance of credentials to DoD entities on the Non-secure Internet Protocol Router Network (NIPRNet), and the External Certification Authority (ECA) program sponsored by DoD issues credentials to contractors and other external partners for interoperability with NIPRNet entities. Although the infrastructure is fielded on the Secret Internet Protocol Router Network (SIPRNet) the infrastructure for certificate issuance is not as widely disseminated as it is on the NIPRNet, making wide use of certificates on the SIPRNet more difficult. In addition, the ability of the DoD PKI to issue credentials to non-human entities is limited to traditional web servers and mobile code signers. Organizations within DoD requiring certificates beyond this, must articulate their needs to the DoD PKI Program Management Office (PMO) for consideration.

An additional issue to be considered is that PKI, as deployed by DoD PKI program, is not identical to PKI as deployed by others, including the intelligence community. Neither are there established trust relationships between the intelligence community and DoD for the acceptance of each other's PKI certificates. The absence of trust agreements between agencies will prevent PKI from directly supporting cross-domain transactions, including transactions involving multi-national information sharing.

Mitigation Approach: NECC will work with the DoD PKI PMO and Combatant Commanders/Services/Agencies (CC/S/A) registration authorities to ensure a robust infrastructure for registering and issuing all required credentials on NIPRNet and SIPRNet. In addition, NECC will identify entities that need PKI credentials that are currently unsupported by DoD PKI. Finally, NECC will involve itself into Federal bridge initiatives to develop trust relationships with organizations outside of the DoD community.

11.2 Accreditation across DAAs

Achieving a secure environment that meets IA requirements and DoD mandates, and integrating IA into SOA are of paramount importance to all DoD WS applications. This is because WS

offer entities access and visibility into DoD's internal Information Technology (IT) architectures, information, and processes. Greater accessibility of data, dynamic application-to-application connections, and lack of a well-defined and bounded run-time environment (provided by WS implementations) introduce significant security risks to DoD's IT environment if not properly managed. NECC will pursue 'type' accreditation for its CMs; however, this accreditation must be accepted by other DAAs in order for NECC to be fielded.

The following is a high-level summary of challenges for achieving IA and accrediting WS-oriented applications in a dynamic operational environment. These issues must be resolved in order to avoid any impact on fielding of new system capabilities.

- **Accreditation Boundaries and System Definitions** – NECC will develop criteria to define boundaries for its WS applications.
- **Dynamic Configuration of Systems** – The DIACAP is not prescriptive on how to accredit a collection of WS applications operating in a dynamic environment, where loosely coupled modules bind and unbind in order to produce capability on an ad hoc and real-time basis. NECC will be a pathfinder to develop these methodologies.
- **No Common Risk Language for Interconnections** – In a WS environment, when faced with verification of security credentials between security domains, varying interpretations of risk will differ between the DAAs for each security domain. Acceptable residual risk for one IA level may not be acceptable for a security domain operating under another IA level. Differing interpretations of residual risk among security domain owners may delay and impede the fielding of new capabilities.
- **Reciprocity** – NECC will embrace the concept of reciprocity as established in the Intelligence Community and DoD C&A goals. This goal seeks to establish cooperation as a normal business practice to facilitate the re-use of systems developed and approved by other organizations. The NECC DAA decisions will support the deployment of NECC software across service boundaries. NECC needs to build an efficient process which uses existing C&A artifacts whenever possible to meet the needs of the NECC certification. The acquisition methodology is an important consideration in this process since a decision to adopt existing software should facilitate the reuse of C&A artifacts and not be limited to the software functions. Reciprocity is an important topic that will be addressed within the NECC C&A Process document.

Mitigation Approach: For Increment 1, NECC has adopted the use of a tailored C&A process to meet the program's needs for C&A. The program will continue to work with the DAA, the certifier, and other IA stakeholders (i.e., PAA and the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG)) to develop processes to ensure the secure enablement of capabilities. NECC will use the FDCE to make the C&A status of all NECC CMs available to all stakeholders reducing uncertainty as to the status of any particular CM. Boundaries for each NECC CM will be established during that module's design.

11.3 NCES Security Services

NECC is planning to use NCES Security Services to implement the authorization function needed to implement access control. However, the NCES program schedule is not fully

synchronized with the NECC program schedule. NCES will develop services to support Attribute-Based Access Control (ABAC) as part of their program, but this will not be complete when the early NECC CMs are ready for fielding. The implementation of a robust ABAC solution also requires the development of new business processes to define attributes, assign authoritative attribute sources, and assign these attributes to people and services.

Mitigation Approach: NECC will work with NCES to develop an integrated program schedule. As required, NECC will identify alternatives and/or limitations while waiting for NCES capabilities. The alternatives include the possible use of a Role-Based Access Control (RBAC) or Access Control Lists (ACL) based upon individual identities. Due to the loosely coupled nature of the SOA, CMs should be able to adopt NCES Security Services rapidly as they become available.

11.4 Cross Domain Solutions

NECC has established requirements to move data between different security domains for both US-only networks and coalition networks. This data movement will rely on CDS. The development of a new CDS is a time consuming process, which takes three years time.

Mitigation Approach: NECC will use CDS developed or in development by other programs to meet NECC cross-domain requirements. The NECC data strategy is to mark NECC data with XML tags using the Intelligence Community Information Security Markings (IC ISM) metadata standard. Current cross-domain guards (examples: Radiant Mercury, Information Support Server Environment guard, and DataSync guard) are being upgraded to handle XML documents, and these upgrades will be useful in the NECC SOA. NECC will form business relationships with programs that develop and host these guards at organizations such as NSA and DISA/IA32. NECC will coordinate its CDS activity with the DoD's Unified Cross Domain Management Office and the Multinational Information Sharing program.

12 POLICY/DIRECTIVES

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005
- CJCSI 6211.02B, *Defense Information System Network (DISN): Policy, Responsibilities and Processes*, 31 July 2003
- CJCSI 6212.01D, *Interoperability and Supportability of National Security Systems (NSS) and Information Technology (IT) Systems*, 8 Mar 06
- CJCSI 6510.01D, *Information Assurance (IA) and Computer Network Defense (CND)*, 15 Jun 04
- DCIO Memo, *Interim DoD Information Assurance Certification and Accreditation Process Guidance (DIACAP)*, July 6, 2006.
- Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program*, Dec 05
- Department of Defense Directive (DoDD) 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 5 May 04

UNCLASSIFIED

- DoDD 5000.1, *The Defense Acquisition System*, 12 May 03
- DoDD 8500.1, *Information Assurance*, 24 Oct 02
- DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, August 15, 2004
- Department of Defense Instruction (DoDI) 4630.8, *Procedures for Interoperability and Supportability of IT and NSS*, 30 Jun 04
- DoDI 5000.2, *Operation of the Defense Acquisition System*, 12 May 03
- DoDI 8110.1, *Multinational Information Sharing Networks Implementation*, 6 Feb 04
- DoDI 8500.2, *Information Assurance Implementation*, 6 Feb 03
- DoDI 8520.2, *Public Key Infrastructure (PKI) and Public Key Enabling (PKE)*, 1 Apr 04
- DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System*, 9 Jul 04
- (U) Information Operations Capstone Threat Assessment, DI-1577-33-06 Volumes 1-15, Jan 06, (Secret/No Foreign (S//NF)//20300804)
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, Jan 00
- *Technology Collection Trends in the U.S. Defense Industry 2002*, Defense Security Service, 23 Oct 02
- 10 U.S.C. Section 2224, *Defense Information Assurance Program*, 18 Mar 04
- Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 5, 1999
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, "National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000

13 RELEVANT ASSOCIATED PROGRAM DOCUMENTS

This NECC Acquisition IAS version reflects these capabilities and program documents:

- NECC Capabilities Development Document (CDD), (Final), 7 June 07
- NECC Information Support Plan (ISP), (Draft 0.03), 27 April 07
- NECC Acquisition Strategy, (Draft 0.3.0), 13 June 07
- NECC Systems Engineering Plan, (Draft 0.7.2), 25 June 07

14 POINTS OF CONTACT

The NECC program is managed by the Defense Information Systems Agency, P.O. Box 4502, Arlington, VA 22204-4502.

**PROGRAM MANAGER /
DISA-NECC**

Laura Knight
Program Manager
Laura.Knight@disa.mil
703 882-2268

PROGRAM CONTROL

Kimberly Davis
Chief, Program Control
Kimberly.Davis@disa.mil
703 882-1269

**IA MANAGER /
NECC-CC12**

Steve Koehler, DISA NECC
NECC Information Assurance
Steve.Koehler@disa.mil
703 882-0297

APPENDIX A – GLOSSARY**ADOPT, BUY, CREATE (ABC)**

During Increment 1, NECC's acquisition approach is to ADOPT proven specifications, best practices, standards, interface definitions, and capabilities; to BUY services through a variety of acquisition mechanisms; and to avoid the CREATION of new services.

CAPABILITY MODULE (CM)

A set of hardware and/or software components that collectively provide a set of logically grouped, operationally relevant services are called CMs. Within NECC, all capabilities will be realized and provided through a set of integrated CMs. Aside from capabilities, CMs are expected to provide a logical access point for every security enclave that they support, thus allowing users to access CMs from within the secure environment in which they are already operating.

CAPABILITY PROVISIONING ACTIVITIES (CPAS)

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

FEDERATED DEVELOPMENT AND CERTIFICATION ENVIRONMENT (FDCE)

The FDCE is a federated development, integration, testing, and certification environment, which has been established by involving DISA, the Services, and COCOMs. It will build on the Net-Centric Engineering Environment (NCEE) Infrastructure, developed for the TD phase, be managed by the NECC team, and be hosted in NECC enterprise facilities. It must provide a hierarchy of environments that match the phases of development, and be a low-barrier, network-accessible environment for learning, exploration, and initial testing. The environment will be a closed, LAN/WAN-based environment for integration, load, and performance testing, and a SIPRNet enclave testing and certification environment for real-world integration and end-user involvement.

GIG COMPUTING NODE (GCN)

The NECC materiel providers will offer their services from a qualified GCN. NECC Increment 1 will use geographically dispersed, military grade enterprise, maritime, and land-based (Government or commercial) GCN. All GCNs must meet tailored availability, security, performance, manageability, and interoperability standards that are consistent with the environment of the GCN.

LOOSELY COUPLED

Loose coupling is a characteristic of the operational relationship between any two entities, but leads to improved dependability, agility, and value of the overall system. This state exists when implementation dependencies between two entities are eliminated in order to maximize the potential for establishing interaction and maintaining that interaction during change.

NET-ENABLED COMMAND CAPABILITY (NECC)

NECC replaces the Global Command and Control System-Joint (GCCS-J) and Service variants as the DoD principal C2 information technology. The objective “mission space” for this capability is defined as the area supporting command capability and C2 activities from the National Military Command System (NMCS) through the Joint Task Force (JTF) and Service/Functional components to unit level commanders. NECC integrates existing and emerging C2 capabilities through an enterprise-based Joint architecture integrating applications and databases to support Joint Warfighters, coalition partners, and agencies responsible for homeland security and defense. The NECC program is a systems integrator, not an equipment system, developed holistically along with parallel improvements in Doctrine, Organization, Training, Leadership, Personnel, and Facilities (DOT_LPF). NECC provides agile C2 capability allowing Joint forces to operate within the adversary's decision cycle by facilitating enhanced battle space awareness, timely information exchange, and net-centric information sharing to support critical Joint and multinational operations.

PROGRAM MANAGEMENT DIRECTION TEAM (PMDT)

The PMDT consists of the JPM, Component Program Managers (CPMs) and their CEs, and subordinate WGs. The PMDT/WGs construct enables collaboration and integration across the technical disciplines, domain knowledge, and stakeholders required for prudent decision making. The JPM, in collaboration with the CPMs, formulates NECC program strategy and execution approaches, which are then presented to the JPEO for approval.

SERVICE LEVEL AGREEMENTS (SLAs)

One of the most critical factors in the success of any outsourcing relationship is the SLA portion of the contract. SLAs are the critical foundation that the service recipient uses to manage the service provider. SLAs are a means of incorporating Performance-Based Service Contracting (PBSC) into software acquisition. An SLA should contain a definition of a service requirement that is both achievable by the provider and affordable by the customer. An SLA is a contractual mechanism between a provider of services and a customer that defines a level of performance. This agreement defines in measurable terms the service to be performed, the level of service that is acceptable, the means to determine if the service is being provided at the agreed upon levels, and incentives for meeting agreed upon service levels. SLAs contain QoS requirements, including how it is to be measured. SLAs also set forth the roles and responsibilities—in contractual form—of both the organization and the provider of the services and products.

APPENDIX B - ACRONYM LIST

Acronym	Definition
ABAC	Attribute-Based Access Control
ABC	Adopt-before-Buy, Buy-before-Create
ACAT	Acquisition Category
ACL	Access Control Lists
ADM	Acquisition Decision Memorandum
AS	Acquisition Strategy
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
C&A	Certification and Accreditation
C2	Command and Control
C2C	Command and Control Capabilities
CA	Certification Authority
CAT	Category
CC/S/A	Combatant Commanders/Services/Agencies
CCB	Configuration Control Board
CDD	Capability Development Document
CDP	Capabilities Definition Package
CDS	Cross-Domain Solutions
CE	Chief Engineer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CL	Confidentiality Level
CM	Capability Modules
CMTT	Capability Module Test Team
CMAR	Capability Module Assessment Reports
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COA	Course of Action
COCOM	Combatant Command
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
CPAS	Capability Provisioning Activities
CPM	Component Program Manager

UNCLASSIFIED

Acronym	Definition
CPMO	Component Program Management Office
CSP	Capability Security Plan
DAA	Designated Accrediting Authority
DCID	Director of Central Intelligence Directive
DECC	Defense Enterprise Computing Center
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIL	Disconnected/Intermittently Connected/Limited Connectivity
DISA	Defense Information Systems Agency
DISA COI	DISA Chief Information Officer
DISN	Defense Information System Network
DISR	DoD Information Technology Standards Registry
DITPR	DoD Information Technology Portfolio Repository
DOT_LPF	Doctrine, Organization, Training, Leadership, Personnel, and Facilities
DSAWG	DISN Security Accreditation Working Group
DT	Developmental Test
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	DoD Intelligence Information Systems
ECA	External Certification Authority
FASA	Federal Acquisition Streamlining Act
FDCE	Federated Development and Certification Environment
FFRDC	Federally Funded Research and Development Center
FISMA	Federal Information Security Management Act
FOC	Full Operational Capability
FOIA	Freedom Of Information Act
FY	Fiscal Year
FoS	Family of Systems
FSO	Field Security Operations
GCCS	Global Command and Control System
GCCS-J	Global Command and Control System-Joint

UNCLASSIFIED

Acronym	Definition
GCN	GIG Computing Node
GIG	Global Information Grid
GOTS	Government-Off-The-Shelf
IA	Information Assurance
IA CAT	Information Assurance Compliance Assessment Tool
IAM	Information Assurance Manager
IAS	Information Assurance Strategy
IC ISM	Intelligence Community Information Security Marking
IDIQ	Indefinite Delivery/Indefinite Quantity
IO CTA	Information Operations Capstone Threat Assessment
ISP	Information Support Plan
ISSE	Information Systems Security Engineer
IT	Information Technology
JC2	Joint Command and Control
JCCD	Joint Combat Capability Developer
JPEO	Joint Program Executive Office
JPM	Joint Program Manager
JPMO	Joint Program Management Office
JST	Joint System Team
JTF	Joint Task Force
LAN	Local Area Network
MAC	Mission Assurance Category
MCP	Mission Capability Package
MIPR	Military Interdepartmental Purchase Request
MS	Milestone
NCEE	Net-Centric Engineering Environment
NCES	Net-Centric Enterprise Services
NECC	Net-Enabled Command Capability
NGA	National Geospatial-Intelligence Agency
NIACAP	National Information Assurance Certification and Accreditation Process
NIPRNet	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMCS	National Military Command System

UNCLASSIFIED

Acronym	Definition
NSA	National Security Agency
NSS	National Security Systems
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OT	Operational Test
OTA	Operational Test Agency
PAA	Principal Accrediting Authority
PBSC	Performance-Based Service Contracting
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PL	Protection Level
PM	Program Manager
PMDT	Program Management Direction Team
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PPSM	Ports, Protocols, and Services Management
QoS	Quality of Service
RBAC	Role Based Access Control
RMP	Risk Management Plan
S//NF	Secret/No Foreign
SAML	Security Assertion Markup Language
SCI	Sensitive Compartmented Information
SDD	System Development and Demonstration
SE	Systems Engineering
SETA	Systems Engineering and Technical Assistance
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreements
SNAC	System and Network Attack Center
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol

UNCLASSIFIED

Acronym	Definition
SP	Special Publication
STA	Surveillance and Target Acquisition
STIGs	Security Technical Implementation Guides
TD	Technology Development
T&E	Test and Evaluation
TEC	Test, Evaluation, and Certification
TEMP	Test and Evaluation Master Plan
TLS	Transport Layer Security
TO	Task Orders
U.S.C	US Code
UDOP	User Defined Operational Picture
USAF	United States Air Force
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
WAN	Wide Area Network
WG	Working Group
WIPT	Working-level Integrated Product Team
WP	Work Packages
WS	Web Services
XML	eXtensible Markup Language