



JOINT REQUIREMENTS
OVERSIGHT COUNCIL

THE JOINT STAFF
WASHINGTON, D.C. 20318-8000

JROCM 173-07
16 July 2007

MEMORANDUM FOR DISTRIBUTION

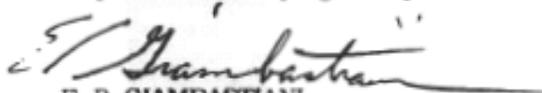
Subject: Net-Enabled Command Capability Increment One Capability
Development Document

1. The Joint Requirements Oversight Council (JROC) approves the Net-Enabled Command Capability (NECC) Increment **One Capability** Development Document and Extensions, and validates the enclosed key performance parameters and key system attributes. The JROC will **maintain approval** authority for all key performance parameter changes, **delegates capability** development document approval authority oversight for changes to key system attributes to the Joint Capabilities Board, and delegates **capability** development document approval authority for all other non-key performance parameter/non-key system attribute changes to USJFCOM via the **Joint Combat Capability Developer** organization as outlined in the capability development document. Capability developers will use the NECC Capability Development Document and Extensions as the initial statement of validated capability needs for all phases of development. This program is assigned the Joint Potential Designator of "JROC Interest."

2. USJFCOM, working in concert with the Services and appropriate agencies, will determine program funding requirements for POM 2010 and beyond.

3. Should the Defense Information Systems Agency encounter costs exceeding ten percent of the approved acquisition program baseline or 25 percent of the original program baseline (Program Acquisition Unit Cost/Acquisition Procurement Unit Cost), they shall return to the JROC prior to reprogramming or budgeting additional funding into the program.

4. The JROC recognizes the importance of the NECC program and requests USJFCOM return to the JROC to provide annual program updates.


E. P. GIAMBASTIANI
Admiral, US Navy
Vice Chairman
of the Joint Chiefs of Staff

Enclosure

UNCLASSIFIED // FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY



**Net-Enabled Command Capability (NECC)
Capability Development Document (CDD)
Linked Extension E – Threat Summary and
Assessment**

Increment: I

7 June 2007

This document has been approved by J8 for release to
Australia, Canada, and Great Britain

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Table Of Contents

1. EXTENSION E - THREAT SUMMARY AND ASSESSMENT..... E-1

1 GENERAL THREATS TO NECC E-1

1.1 INFORMATION OPERATIONS (IO) THREATE-1

1.2 COALITION-RELATED THREAT.....E-2

1.3 COMPUTER NETWORK ATTACK (CNA)/COMPUTER NETWORK EXPLOITATION (CNE) E-2

1.4 THREAT ASSESSMENT DOCUMENTS.....E-2

Foreign Releaseability

This document is authorized for release (either hardcopy or electronically) to Australia, Canada, and Great Britain governments and their respective contractors and representatives working as mutual defense cooperative capability partners in support of NECC.

AUS, CAN, GBR government agencies and their defense support contractors may disseminate “For Official Use Only” information to their employees and subcontractors who have a need for the information. Removal of the “For Official Use Only” marking can only be accomplished by the USJFCOM J88. All “For Official Use Only” information shall be stored in locked receptacles such as file cabinets, desks, or bookcases. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection. During working hours, the information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. Transmission of “For Official Use Only” information may only be accomplished on a government-to-government basis.

Further requests for this document should be submitted to:

**Joint Combat Capability Developer (J88)
U.S. Joint Forces Command
1562 Mitscher Avenue, Suite 200
Norfolk, Virginia 23551-2488**

Points of Contact

John Wellman, NECC JCCD Lead, J88 USJFCOM, (757) 836-0126, john.wellman@jfc.com

John Costello, NECC Washington Liaison Office Lead, J882DC USJFCOM, (703) 614-5016, john.costello@jfc.com

John Nankervis, NECC Capability Development & DOTMLPF Lead, J882B USJFCOM, (757) 836-6310, john.nankervis@jfc.com

Extension E - Threat Summary and Assessment

1 General Threats to NECC

As the NECC community migrates to a net-centric environment, NECC architecture must ensure secure, seamless exchange of information and implement safeguards to defend and protect against unauthorized external/internal access to its MCPs and associated Service/Agency/joint-provided data sources. NECC must support information exchange across multiple security domains between elements of the NECC community while defending against attacks from the low side and preventing leakage of data from high-to-low domains.

1.1 Information Operations (IO) Threat

As the C2 capability for the DOD, NECC will likely be targeted for direct or indirect attacks as will associated Service, Agency, or joint-provided data sources. The primary threat to any C2 system like NECC is that of adversarial information operations (IO). IO is defined as actions taken to affect adversary information and information systems while defending one's own information and information systems. IO requires the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. Major capabilities to conduct IO include electronic warfare (EW), computer network operations (CNO), foreign influence operations (FIO), denial and deception (D&D), and physical attack or destruction. By employing these IO techniques in a concerted manner, an adversary could degrade the entire information chain vital to NECC.

Adversaries recognize our civilian and military reliance on advanced information technologies and systems and understand information superiority provides the US with unique advantages. Accordingly, potential foes could pursue IO to counter US superiority by attacking NECC. For example, adversarial use of EW, FIO and D&D against sensors and systems feeding NECC could negatively affect the quality of data used by decision makers.

Additional threats may involve denial of service by limiting or disrupting access to data sources. Denial of service may come from data-driven attacks by foreign adversaries or terrorists who attempt to disrupt joint and multinational operations or by internal failures to process transactions in a timely manner.

Because NECC uses COTS products, widely available IO attack tools are increasingly capable of being used by those less technically skilled. Integration of COTS products and seamless services in NECC will require close scrutiny during development and implementation to maximize exploitation of commercial products while retaining the requisite level of security.

Opponents that have knowledge of NECC architecture and interfaces may be able to exploit and attack NECC program capabilities. DOD systems are regularly probed and scanned to determine network architectures and assess vulnerabilities as prerequisites to exploitation and/or attack, via foreign locations. Physical attack may also be used against NECC personnel, facilities, and hardware.

1.2 Coalition-Related Threat

Threats to allies may become a threat to NECC, even when it's not the primary target. Connectivity and interoperability between DOD and coalition, allied, and non-allied users and systems suggest an increasing number of potential insider threats.

1.3 Computer Network Attack (CNA)/Computer Network Exploitation (CNE)

An adversary's employment of CNO techniques, especially computer network exploitation (CNE) and computer network attack (CNA), could degrade the automated information systems (AIS) on which NECC relies. In general, implementing the Defense-in-Depth strategy and related Operations Security (OPSEC) methodologies will reduce vulnerability and minimize adverse mission impact to threats discussed above.

Continued efforts are required to integrate CNA&CNE capabilities within the GIG (including NECC and Net-centric Enterprise Services (NCES)) to effectively protect and defend against IO threats and exploit the enemy's systems and decision cycle. Central to an effective, state of the art, defense-in-depth strategy, is the capability to scan for cyber attacks.

CNA and CNE include, but are not limited to: stealing passwords and data, inserting malicious code, denial of services, and data corruption, modification, and manipulation. CNA and CNE tactics could potentially be used against computer systems and software applications of NECC.

The GIG must be compatible with Information Assurance & Vulnerability Assessment (IAVA) compliance and Information Assurance Vulnerability Management (IAVM) system per DODD 8500.1. GIG components must be National Information Assurance Partnership (NIAP) compliant. NIAP is a partnership between the National Institute of Standards & Technology (NIST) and National Security Agency (NSA) for evaluating information technology security products.

A minimum degree of degradation can be achieved through the GIG's modular architecture. In case of attack, individual effected modules will be shut down without affecting the entire capability.

As the C2 capability for the DOD, NECC will likely be targeted for direct or indirect attacks as will associated Service, Agency, or joint-provided data sources. Most threats are addressed in Defense Intelligence Agency (DIA) published documents listed below and will serve as the DIA-validated baseline for all threats. DIA validated document are denoted by **.

1.4 Threat Assessment Documents

Additional relevant threat assessment documents include:

- (U) Chemical, Biological, and Radiological Warfare Capstone Threat Assessment (U), DI-1650-83-06, June 2006, (S//FGI GBR//NF//MR)
- (U) Information Operations Capstone Threat Assessment, (IO-CTA) 5th Edition (U) DI-1577-33-05, 16 Volumes, January 2006, (S//NF)**
- (U) National Intelligence Estimate on the Cyber Threat to the U.S. Information Infrastructure, NIE 2004-01D/I, February 2004, (S//NF)

UNCLASSIFIED // FOR OFFICIAL USE ONLY

- (U) Naval Electronics, Navigation, and Network Systems (NENNS) Capstone System Threat Assessment (CSTA), ONI-CTA-005-06, September 2006, (S//NF)
- (U) Space Capstone Threat Capabilities Assessment, DoD-1574-0727-06, March 2006, (S//FGI//NF//MR).**