DEPARTMENT OF THE NAVY
CHIEF OF NAVAL AIR TRAINING
CNATRA
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5231.3A
N6
01 AUG 2005

CNATRA INSTRUCTION 5231.3A

Subj: CNATRA INFORMATION SYSTEMS LIFE CYCLE MANAGEMENT FOR NAVY MARINE CORPS INTRANET (NMCI)

Ref: (a) Computer Security Act of 1987 (Public Law 100-235)
(b) OMB Circular A-123
(c) OMB Circular A-130
(d) DODD 8500.1
(e) DODI 8500.2
(f) DOD 5500.7-R
(g) DODI 5200.40
(h) FY 2001 Defense Authorization Act of 2000 (Public Law 106-398) see Title X, Section 2224, DOD IA Program, Government Information Security Reform
(i) OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
(j) Public Law 104-106, National Defense Authorization Act of 1996, Sections D and E, which have been renamed as the Clinger-Cohen Act of 1996
(k) CNATRAINST 5000.2C (R

Encl: (1) NMCI contract N00024-00-D-6000 background
(2) List of Web Links to References and Glossary

1. Purpose

a. To provide policy and guidelines for the Command Information Systems (IS) Life Cycle Management (LCM) and to establish and implement the Program for Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) to meet the requirements of references (a) through (k) upon the implementation of Navy Marine Corps Intranet (NMCI).

b. To define the organizational structure of Information Systems (IS) and Life Cycle Management (LCM) Program.

c. To issue policies and guidelines necessary for consistent and effective implementation throughout CNATRA and NATRACOM.

d. To apply basic policy and principles of computer hardware and software management as they relate to Information Management and Information Technology (IMIT) and Information Systems (IS) associated with or connected to the CNATRA and NATRACOM Networks for NMCI.

A) 2. Cancellation. CNATRAINST 5231.3 and NRSINST 5231.1. The focus of this revision is to separate the joint CNATRA/NRS instruction. The only revision markings used are to show other modifications.

3. Background. For a short background and transition synopsis of the Navy-Marine Corps Intranet (NMCI) contract number N00024-00-D-6000, which was awarded by the Navy to Electronic Data Systems (EDS) on October 6, 2000, please refer to enclosure (1) for details. The contract is to build and maintain a secure world-wide network that will provide data, voice, video, and support capabilities to every Sailor, Marine and DON Civilian.

4. Objective. To provide guidelines for IS requirements and LCM support under NMCI.

5. Authority. The CNATRA Command Information Officer (CIO) is responsible for ensuring compliance with the DON Information Systems (IS) Life Cycle Management (LCM) Program under NMCI. The procedures and principles presented in these guidelines apply to all CNATRA and NATRACOM military and civilian employees (including government contractors) and all IT assets within CNATRA and NATRACOM claimancy.

6. Policy

a. After implementation of NMCI, EDS Information Strike Force (ISF) team will furnish new hardware/software to each user. Ownership of existing DON equipment will be relinquished and change hands to the EDS ISF team, with a few exceptions for locally developed legacy-unique systems which are required by the mission whose connectivity has been certified and is residing on local servers. Support may or may not be under a Contract Line Item Number (CLIN) and Service Level Agreements (SLA).

b. Initial NMCI assets in terms of hardware, software and support are determined for users' requirements by CNATRA CIO. A mission inventory analysis is furnished to the Information Strike Force (ISF) team for review and implementation in NMCI. Seats are allotted to users for interoperability and mission

requirements. After system installation, a user may have two (2) moves, add, change (MAC) per year without a fee.

c. User support is provided for hardware/software/support issues by a central point of contact and resolved by EDS contractor personnel on-site. User on-line training is provided on the web as part of the contract.

d. Hardware refresh (upgrades) are executed by EDS after 3 years. Software refresh (upgrades) are executed by EDS upon version changes and updated within a 3-month window period. NMCI equipment inventory and accreditation are executed by the ISF team. The Commander of the Task Force (CTF) is the NMCI Designated Approving Authority (DAA).

e. All NMCI related documentation will flow from unit to respective Activity Customer Technical Representative (ACTR), to Deputy Customer Technical Representative (DCTR), then to CNATRA CIO. Any moves, adds, changes (MAC) that are required by users in terms of mission requirements for hardware, software, data, video, and support will be coordinated with an IT Acquisition Paper (ITAP) thru the local chain to ACTR, DCTR, then to CNATRA CIO for review and approval or disapproval. The ITAP form is documented in reference (k), paragraph 7. A copy of the form is available on the CNATRA website at https://cnatra.navaltx.navy.mil/cnatra/instruct.htm at enclosure (1) (R of reference (k).

f. Requirements will be analyzed and matched with respective NMCI CLINs and SLAs. Since this is a fee-for-service billed by EDS on a monthly basis per requirement, any MAC or additional support requirements will be reviewed on a case-by-case basis.

7. Responsibility. CNATRA CIO is the official authority for NMCI for CNATRA and NATRACOM units. All actions and documentations relative to NMCI will be channeled and coordinated through the CNATRA CIO office. Unit Commanding Officers will implement this policy and guidance within their commands upon NMCI implementation.

R) 8. Contact Information for CNATRA CIO: CNATRA (N6), 250 Lexington Boulevard, Suite 102, Corpus Christi, TX 78419-5041, DSN 861-1430 or Commercial (361)961-1430.

D. B. Grimland

D. B. GRIMLAND
Chief of Staff

Distribution:
CNATRAINST 5215.1R
List I

Copy to:
COMTRAWING TWO (COOP File)
NETC

NMCI BACKGROUND AND TRANSITION SYNOPSIS

1. On October 6, 2000, the United States Navy and Marine Corps awarded a long term contract N00024-00-D-6000 to a single commercial contractor, Electronic Data Systems (EDS), to build and maintain a secure world-wide network that will provide data, voice, video, and support capabilities to every Sailor, Marine and DON Civilian. The contract is known by its acronym as NMCI and stands for Navy Marine Corps Intranet (NMCI). It is intended to eliminate stovepipe systems and modernize the way DON and Marine Corps do business. It will get the government out of owning and operating information technology systems and transfer these functions to a fee-for-service performance-based contract with the private sector. The contract is mandatory for all DON and Marine Corps activities.

2. Chief of Naval Operations (CNO) OPNAV N6 has formed a Commander Task Force NMCI (CTF NMCI) to manage the project under the auspices of the Program Executive Officer (Information Technology) (PEO-IT). CTF NMCI will be responsible for NMCI operations for the Navy; and the USMC Director of Command, Control, Communications, and Computers (C4) will be responsible for operations on the Marine Corps side.

3. The mission of NMCI is to enable the sharing of information worldwide with those who need it, when they need it, and enhance the enterprise-wide work, training, and quality of life for every Marine, Sailor, and DON Civilian. EDS formed an Information Strike Force (ISF) team for transition, conversion, and implementation phases of users seats at installations for the entire DON and Marine Corps ashore and overseas at CONUS, Alaska, Hawaii, Guantanamo Bay (Cuba), Puerto Rico, and Iceland. The transition approach for the implementation of NMCI is designed in five (5) phases with the following approximate timelines:

a. Phase 1 - Workforce Development (1 month).

b. Phase 2a – Detailed Engineering/Design and Build (3 months).

c. Phase 2b - Equipment Transformation/Service Transition (3 months) ”cut over phase”; EDS will start assessing existing desktops.

d. Phase 3 – Achieving and Testing service level agreement (SLAs)(2 months). Initial Operation Capability (IOC) starts at the beginning of Phase 3.

e. Phase 4 - Continuous Improvement/Optimize.

f. Phase 5 - Feedback/Production.

4. Users' seat management concept includes hardware, software, data, video, connectivity, and support capabilities. It encompasses the PC, network, security hardware and software, hardware/software maintenance, hardware/software refresh, e-mail, Web access, two unclassified user accounts, LAN/WAN/MAN connectivity, Non-Classified Internet Protocol Router Network (NIPRNET) (unclassified) or Secret Internet Protocol Router Network (SIPRNET) (classified) access, Help Desk support, desk-side support, shared network printing, network file sharing, directory services, training. It includes 50MB e-mail/calendar storage per account and 200MB network personal file storage per account.

5. There are various seat types: Gold disk, fixed workstations (red, white, blue, thin client); portable (basic or high end); and embarkables (full and limited). Upgrades such as: high-end, mission critical, or classified connectivity are available for some of the seats. The specifications of the seats are available on the NMCI home page web site at enclosure (2). IT hardware technology will be refreshed every three years by EDS. The software updates will be refreshed by EDS as new version(s) are released by software manufacturers.

6. Aviation Training Classrooms, mission support software requirements and designs, development and system analysis tests, as well as certain legacy systems support will be in enclaves of NMCI Community of Interests (COI). They are logical groupings of users who have a requirement to access information that should not be made available to the general NMCI user population. Logical perimeters are established around the COI, using Defense in-Depth Information Assurance (IA) mechanisms, security management and operational directions and will be separated from NMCI at large through Boundary Firewall suites.

7. Boundary 2 Firewall suites providing this function will mirror the NMCI solution for meeting Boundary 1 security requirements. Firewalls are a collection of hardware and software components that are used to provide protection for a defined set of users in a specified enclave. An example for primary entry points protection to external networks such as NIPRNET has been established by DON as Boundary 1. Under the Defense-in-Depth approach, Firewalls should be implemented at multiple layers (Regional, Metropolitan Area Network (MAN), Base Area Network (BAN), Local Area Network (LAN), etc.) to provide

additional layers of protection. Thus, Firewalls can be at Boundary Transport (BT) and Boundaries 1, 2, 3, and 4. Defense-in-Depth boundaries are defined as follows:

a. Boundary Transport (BT), protects areas between NMCI, Transport Wide Area Network (WAN) and Remote NMCI Users.

b. Boundary 1 (B1), protects areas between NMCI users and services located in DON Networks NIPRNET/SIPRNET) and external Internet.

c. Boundary 2 (B2), protects area between NMCI and users/applications located in DON legacy networks.

d. Boundary 3 (B3), protects areas between NMCI Community of Interest(s) (COI) and NMCI.

e. Boundary 4 (B4), protects areas between NMCI Hosts and Servers.

8. Training Classrooms hardware, software and maintenance are procured and refreshed using NMCI CLINs or separate established contract vehicles.

BLANK PAGE

WEB LINKS TO REFERENCES AND GLOSSARY

Computer Security Act of 1987 (Public Law 100-235)
http://www.fas.org/offdocs/laes/pl100235.htm

OMB Circular A-123
http://www.whitehouse.gov/omb/circulars/a123/a123.html

OMB Circular A-130 of 8 Feb 96
http://www.whitehouse.gov/omb/circulars/a130/a130.html
DOD 8500.1 as of 24 Oct 02 (Information Assurance (IA))

http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

DODI 8500.2 as of 6 Mar 03 (IA Implementation)
http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

DOD 5500.7-R of 30 Aug 93 (Joint Ethics Regulation)
http://www.defenselink.mil/dodgc/defense_ethics/

DODI 5200.40 of 30 Dec 97 (DITSCAP)
http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

FY 2001 Defense Authorization Act of 2000 (Public Law 106-398) see Title X, Section 2224, DOD IA Program, Government Information Security Reform
http://www.fas.org/asmp/resources/govern/s1059_106-pl.htm

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

OMB Circular A-130, Transmittal Memorandum No. 4, Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Public Law 104-106, National Defense Authorization Act of 1996 (Section D and E, renamed as Clinger-Cohen Act of 1996)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104.pdf

NMCI HOME PAGE
http://www.nmci-isf.com

NMCI CLIN INDEX
http://www.nmci-isf.com/clinlist.htm

NMCI SLA INDEX
http://www.nmci-isf.com/clin_matrix.xls

NMCI MASTER GLOSSARY OF ACRONYMS
http://www.eds-gov.com/nmcifaqs/master_glossary_of_acronyms.doc