

DEPARTMENT OF THE NAVY
COMMANDER, NAVY REGION SOUTH
CORPUS CHRISTI, TEXAS 78419-5200

CHIEF OF NAVAL AIR TRAINING
CORPUS CHRISTI, TEXAS 78419-5041

NRSINST 5231.2
CNATRAINST 5231.4
N6

21 NOV 2003

NRS INSTRUCTION 5231.2
CNATRA INSTRUCTION 5231.4

Subj: CNATRA-NRS INFORMATION SYSTEMS LIFE CYCLE MANAGEMENT
FOR LEGACY SYSTEMS (NON-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) NRSINST 5000.1A/CNATRAINST 5000.2A
(l) NRSTINST 5200.1/CNATRAINST 5200.7
(m) OPNAVINST 5239.1B
(n) NAVY IA PUB 5239-13
(o) NAVY IA PUB 5239-16

Encl: (1) List of Web Links to References and Glossary
(2) Information on Accreditation Formats

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)-Navy Region South (NRS) and Naval Air Training Command (NATRACOM) to meet the requirements of references (a)

21 November 2003

through (o) for non-Navy Marine Corps Intranet (NMCI) Legacy systems.

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-NRS 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, connected to the CNATRA-NRS and NATRACOM Networks for non-NMCI Legacy systems.

2. Background. As the majority of mission essential application systems are transitioned to NMCI, some applications, equally mission essential application systems have not, due to various reasons. Chiefly among them, these Legacy systems cannot be converted in time to Commercial Off-The-Shelf (COTS) software or Government Off-The-Shelf (GOTS) software during the NMCI conversion or are expected to be converted to other system applications and eventually be included in the NMCI environment. These Legacy systems will continue to be operational either within a quarantine type of Community of Interest (COI) environment within NMCI or stand alone environment, until phased out by management review or merged into newer applications that will be compliant with NMCI standards.

3. Objective. To provide guidelines for IS requirements and LCM support for legacy systems.

4. Authority. The CNATRA-NRS Command Information Officer (CIO), as the Designated Approval Authority (DAA), is responsible for ensuring compliance with the DON Information Systems (IS) Life Cycle Management (LCM) Program for Legacy systems for non-NMCI systems. The procedures and principles presented in these guidelines apply to all CNATRA-NRS and NATRACOM military and civilian employees (including government contractors) and all Information Technology (IT) assets within CNATRA-NRS and NATRACOM claimancy.

5. Policy

a. After implementation of NMCI, Electronic Data Systems (EDS) contractor Information Strike Force (ISF) team will

21 November 2003

furnish new hardware/software to each user and ownership of existing DON equipment will be relinquished and changed 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 residing on local servers. Some Legacy support may be under a Contract Line Item Number (CLIN) and Service Level Agreements (SLA). Remainder of Legacy equipment and application systems will be maintained by a local contractor, under separate contract.

b. Initial NMCI assets in terms of hardware, software and support are determined for user(s) requirements by CNATRA-NRS CIO. A mission inventory analysis is furnished to the Information Strike Force (ISF) team for review and implementation in NMCI. Legacy systems will be reviewed and authorized by the CIO, on a case-by-case basis with respective Commanding Officers or Department Heads.

c. Local Legacy user support is provided for Hardware, software, support issues by a respective central point of contact and resolved by local contractor personnel on-site.

d. Legacy hardware refresh (upgrades) are executed by local contractor personnel, as required, by the contract or after 3 years. Legacy software refresh (upgrades) are executed by local contractor personnel upon version changes or updated within a 3 months window period. The CIO is the Designated Approving Authority (DAA) for system accreditations and Interim Authority to Operate (IATO).

e. All Legacy equipment and applications must be accredited or have an IATO in order to operate the system. Accreditation and Risk Assessment formats are found at enclosure (2). The Risk Assessment formats are also available from your respective Activity Customer Technical Representative (ACTR) in electronic format. Users are to report accreditations to respective ACTRs for consolidation and approval by the CIO. Accreditation copies will be maintained at the user level, ACTR and CIO offices. Initial accreditation packages and annual reviews are due on 30 September of every year by all units to the CIO office. All IATO will be reviewed after 90 days for accreditation compliance.

f. All legacy related documentation will flow from respective Commanding Officers (CO) or Department Heads, to respective ACTR, to Regional Deputy Customer Technical Representative (DCTR), with copy to CIO N611 (Plans & Policy),

NRSINST 5231.2
CNATRINST 5231.4

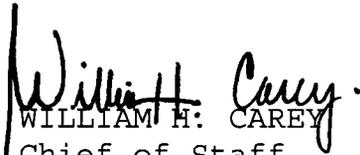
21 NOV 2003

then to CNATRA-NRS CIO. Any updates or upgrades that are required by users in terms of mission requirements for hardware, software, data, video and support will be coordinated with an Information Technology Acquisition Paper (ITAP) thru the local chain to ACTR, DCTR, CIO N611, then to CNATRA-NRS CIO for review and approval or disapproval. ITAP form is found in reference (k), enclosure (1). Equipment, software or personnel changes of Legacy users will be documented with a new accreditation request to ACTR and forwarded for approval.

g. Requirements will be analyzed and matched with respective CNATRA-NRS mission and reviewed on a case-by-case basis.

6. Responsibility. CNATRA-NRS CIO is the official authority for Legacy systems for CNATRA-NRS and NATRACOM units. All actions and documentations relative to Legacy systems will be channeled and coordinated through the CNATRA-NRS CIO office. Commanding Officers will implement this policy and guidance within their commands.

7. Name, address, phone numbers and e-mail of CNATRA-NRS CIO:
Mr. Thomas Albro, CNATRA-NRS CIO, Code N6, 250 Lexington Boulevard, Suite 265, Corpus Christi, TX 78419-5041, DSN 861-1430 or (361) 961-1430 and e-mail: Thomas.albro@nrs.navy.mil


WILLIAM H. CAREY
Chief of Staff

Distribution:
CNATRINST 5215.1R
List I
List III
NS Ingleside
NRS RBO

Copy to:
COMTRAWING TWO (COOP File)
NETC

21 November 2003

WEB LINKS TO REFERENCES

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

NRSINST 5231.2
CNATRAINST 5231.4

21 November 2003

Respective CNATRA-NRS Instructions are available at
<https://cnatra.navaltx.navy.mil/cnatra/instruct.htm>

NMCI MASTER GLOSSARY OR ACRONYMS

http://www.eds.gov/nmcifags/master_glossary_of_acronyms.doc

OPNAVINST 5239.1B

http://neds.nebt.daps.mil/Directives/5239_1b.pdf

NAVY IA PUB 5239-13 (VOL 1, II, III) and NAVY IA PUBS 5239-16

<https://www.infosec.navy.mil/content.html>

21 November 2003

**Accreditation Request for Single/Multiple Computers
of the Same Architecture and Configuration**

Index of Accreditation and Risk Assessment formats:

Part I - Accreditation Request

Part IIa - Risk Assessment (Generic)

Part IIb - Risk Assessment (Win NT)

Part IIc - Risk Assessment (Win2000)

Part IID - Risk Assessment (Palm/PDA)

Part IIIa - Risk Assessment (Classified processing)

Part IIIb - Risk Assessment (Classified network)

Part IIIc - Risk Assessment (Firewall)

Part IVa - Risk Assessment (E-mail server)

Part IVb - Risk Assessment (Web server)

1. Select Part I in this section - to be filled out by all legacy system users (military, civilians and contractors). After completing it, go to paragraph 2, below. Users must identify all Legacy systems associated with equipment used (desktop/laptop) and software).

2. Select appropriate Part II with corresponding line(s) in this section, depending on systems used. To be filled out by all users, with assistance by Network administrators, Activity Customer Technical Representative (ACTR), Information Systems Security Manager (ISSM). If no classified data is processed go to paragraph 5 below, otherwise go to paragraph 3, below.

3. Select appropriate Part III and corresponding line(s) in this section, depending on systems used. To be filled out by users, with assistance by Network administrators, ACTR, ISSM. Go to paragraph 4, below.

4. Select appropriate Part IV and corresponding line(s) in this section, depending on systems used. To be filled out by Network administrators, ACTR, ISSM. Then go to paragraph 5, below.

5. Provide **all** accreditation documentation(s) to respective ACTR for review then forward to DCTR. DCTR will forward to CIO office N611 then to CIO for final approval or disapproval. Incomplete documentation will be returned to DCTR/ACTR.

Enclosure (2)

NRSINST 5231.2
CNATRAINST 5231.4

21 November 2003

Respective formats are available at URL below and from the respective ACTRs.

<http://cnatra.navaltx.navy.mil/cnatra/roger/RISK%20ASSESSMENT%20FORMATS%202003.doc>