DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

CNICINST 5239.1A
N6
13 Jun 2012

CNIC INSTRUCTION 5239.1A

From: Commander, Navy Installations Command

Subj: CNIC INFORMATION ASSURANCE PROGRAM

Ref: (a) DoD Directive O-8530.1 of 8 Jan 2001
(b) DoD Directive 8570.01 of 15 Aug 2004
(c) DoD 8570.01-M of 20 Apr 2010
(d) Public Law 107-347, Federal Information Security Management Act of 2002, Title III of E-Government Act of 2002
(e) SECNAVINST 5239.3B
(f) DoD Instruction 8500.2 of 6 Feb 2003
(g) DoD Directive 8500.1E of 24 Oct 2002
(h) DoD Information Assurance Certification and Accreditation Process Handbook Version 1.0
(i) DON CIO Memo 02-10
(j) DoD Instruction 8510.01 of 28 Nov 2007
(k) CJCS Instruction 6510.01F

Encl: (1) CNIC Information Assurance Policy

1. Purpose. To revise the information assurance (IA) program in accordance with references (a) through (k) through the issuance of Commander, Navy Installations Command (CNIC) Information Assurance policy.

2. Cancellation. CNICINST 5239.1 dated 30 Oct 2008.

3. Background. The CNIC IA program incorporates processes to educate and certify command personnel responsible for information security within the command; establishes a requirement for self-inspection and continuous monitoring of application, network and system security; executes a process for certification and accreditation of CNIC networks and systems in accordance with reference (h); amplifies and reinforces command compliance with higher level IA guidance.

4. Policy. This instruction delivers the policy upon which the IA program is implemented throughout CNIC.

a. CNIC IA Policy. Enclosure (1) is the framework for enabling secure access to mission critical information and CNIC information technology (IT) services; ensuring availability and protection of CNIC data and networks; and organizing resources to quickly mobilize and re-establish CNIC IT services in the event of attack or compromise.

b. Standard Operating Procedures & Templates. The processes to be executed in support of the CNIC IA policy are available on the CNIC Gateway 2.0 Information Assurance (N64) teamsite at: https://g2.cnic.navy.mil/TSCNICHQ/N6/N64/default.aspx.

5. Responsibilities. CNIC Information Technology Services (N6) is responsible for reviewing the effectiveness of the IA program and enhancing the policy and program to coincide with evolving Department of Defense, Department of Navy and Federal cyber initiatives and information security strategy.

6. Action

a. CNIC Commander, Deputy Commander, Region Commanders, Command Information Officer (CIO), IA Program Managers (IAPMs), IA Managers (IAMs), and IA Officer (IAOs) shall execute responsibilities as outlined in section 3 of enclosure (1) of this policy.

b. CNIC CIO, Region CIOs, and HQ/Region/Site IAPM shall complete actions as outlined in section 4 of enclosure (1) of this policy.

W. D. FRENCH
Vice Admiral, U.S. Navy

Distribution:
Electronic only, via Gateway 2.0
https://g2.cnic.navy.mil/CNICHQ/Pages/Default.aspx

CNIC INFORMATION ASSURANCE POLICY

1. Applicability

a. This policy and the responsibilities detailed herein apply to all Commander, Navy Installations Command (CNIC) personnel including civilian, contractor, military and non-appropriated fund personnel that administer, defend, develop, maintain, operate, use or retire information technology (IT) systems and services under the operational control of CNIC.

b. The provisions set forth in this policy are to be initiated and enforced at the Echelon II and cascaded down to all subsequent command levels as applicable.

c. This policy supplements the information assurance (IA) policy established by reference (e). The CNIC IA policy is not intended to replace the higher level instruction. If a question arises regarding the applicability or execution of this policy the matter shall be escalated to the CNIC Command Information Officer (CIO), via the chain of command, for resolution.

2. CNIC Information Assurance Program

a. IA Awareness Training.

(1) As a condition of IT access, all CNIC personnel shall be required to complete Department of Defense (DoD)-approved IA awareness orientation and subsequently required to complete annual refresher IA training in accordance with reference (b). The IA awareness training records will be maintained in Total Workforce Management Services (TWMS). Additional information is available on the CNIC Gateway 2.0 (G2) Information Assurance (N64) teamsite at: https://g2.cnic.navy.mil/TSCNICHQ/N6/N64/default.aspx.

b. IA Workforce Management.

(1) CNIC personnel performing IA tasks or assigned IA job functions, in accordance with reference (c), shall be formally identified as IA workforce.

(2) CNIC IA workforce shall comply with the qualifications, certification and training requirements set forth in reference (c).

(3) CNIC maintains a CNIC IA Workforce Improvement Program (WIP) manual that details CNIC roles and responsibilities to be accomplished in accordance with reference (b). The CNIC WIP is available on the G2 IA (N64) teamsite.

c. Defense in Depth. The CNIC IA program shall incorporate controls to comply with the DoD defense-in-depth strategy set forth in reference(e).

d. Certification & Accreditation. In accordance with DoD Information Assurance Certification and Accreditation Process (DIACAP) and Federal Information Security Management Act (FISMA) requirements CNIC systems shall be certified and accredited as a condition of connection to the Global Information Grid (GIG). Systems identified as Platform-IT (PIT) shall comply with DIACAP per Fleet Cyber Command (FLTCYBERCOM) guidance. The PIT process is available on the G2 IA (N64) teamsite.

e. Incident Management. CNIC shall establish a CNIC Cyber Security Operations Center (CSOC) to centrally manage and monitor CNIC Host-Based Security Systems (HBSS).

(1) Incidents that occur on these systems will be analyzed by the CNIC CSOC and reported to the Navy Cyber Defense Operations Command (NCDOC) via CNIC N64. CNIC N64 shall ensure timely handling of signature threshold alerts, updates, and audit records and log files.

(2) The HBSS shall be configured in accordance with current guidance provided by FLTCYBERCOM and USCYBERCOM.

3. Responsibilities

a. The CNIC Commander in collaboration with the CNIC Deputy Commander is responsible for appointing a CNIC Command Information Officer (CIO) to direct and oversee the implementation of the CNIC IA program.

b. The Region Commanders are responsible for designating CIOs to implement and manage the CNIC Information Assurance program throughout CNIC commands. The Region and Installation CIOs shall receive operational direction from the CNIC CIO.

c. The CNIC CIO is responsible for designating an Information Assurance Program Manager (IAPM) to implement the

CNIC IA policy and administer the CNIC IA program. The IAPM designation shall be presented in writing to the Echelon II.

d. The IAPM is responsible for providing operational direction, under the supervision of the CNIC CIO, to Region CIOs and IA Managers as it relates to the compliance, execution and enforcement of the CNIC IA policy and higher level information assurance governance.

e. The IT project manager, with input from the Region CIO, is responsible for appointing in writing Information Assurance Managers (IAMs) and Information Assurance Officers (IAOs).

f. The IAM is responsible for reinforcing the tenets of the CNIC IA policy within the designated role of responsibility.

g. The IAO is responsible for ensuring the IT system addresses prescribed IA requirements and maintains an approved authorization to operate. A template for the appointment is available on the G2 IA (N64) teamsite.

4. Actions.

a. CNIC CIO shall:

(1) Incorporate a mission objective for IA as part of the CNIC IT strategy and reinforce the IA management as a strategic priority throughout the lifecycle of all CNIC IT programs.

(2) Develop CNIC IA policy that supplements higher level policy and institute CNIC-specific standards, practices and processes that mitigate the risk and potential harm that could result from unauthorized disclosure, disruption, modification or destruction of information assets within CNIC.

(3) Implement IA policy throughout the CNIC command.

(4) Mandate continuous security monitoring for all CNIC IT programs to include vulnerability assessments, threat modeling, and penetration testing.

(5) Utilize a Security Assessment Team (SAT) to visit command sites for the purpose of discovery, inspection, certification and accreditation assistance, and incident response.

(6) Direct the creation and management of a CNIC Security Operations Center.

(7) Direct the IAPM to reinforce IA awareness training for all CNIC personnel.

(8) Enforce the DoD certification and training requirements for all CNIC personnel identified as IA Workforce.

(9) Ensure IA policy is executed and enforced throughout CNIC Regions in accordance with DoD, DON and Federal IA directives.

(10) Deliver facts, figures and metrics in response to IA reporting requirements requested by DoD, DON and Federal authorities.

(11) Evaluate annually the effectiveness of the CNIC IA program in accordance with FISMA and provide input to DON CIO for collective annual reporting on information security.

(12) Endorse the sustainment and supportability of all CNIC IT assets to include IA compliance.

(13) Integrate IA into CNIC IT strategic planning and system acquisition management. Align CNIC IT strategic planning and system acquisition management with DoD policy.

(14) Establish a committee to review the IA strategy for major acquisition programs as part of managing IT investments.

(15) Coordinate CNIC response FLTCYBERCOM and NCDOC on IA matters and Computer Network Defense (CND) issues.

(16) Ensure compliance with reference (e).

b. Region CIOs shall perform the CIO duties specified for the CNIC CIO commensurate with his/her command level and with the intent to avoid redundancy in the execution of these duties.

c. Headquarters (HQ) IAPM shall:

(1) Take direction from the CNIC CIO as it relates to management of the CNIC IA program.

(2) The IAPM will serve as a subject matter expert on all information assurance matters.

(3) Perform the duties of the role as defined in the CNIC Information Assurance Workforce Improvement Program Manual. The manual is available on the G2 IA (N64) teamsite.

(4) Administer the CNIC IA program.

(5) Develop procedure in support of CNIC IA policy.

(6) Direct SAT efforts in accordance with the protocol established in the SAT standard operating procedure (SOP). The SOP is available on the G2 IA (N64) teamsite.

(7) Facilitate collaboration and communication between the Programs, Regions, Office of Designated Accrediting Authority (ODAA) and Navy Certifying Authority.

(8) Coordinate IA incident reporting to NCDOC and FLTCYBERCOM in accordance with the incident reporting SOP. The SOP is available on the G2 IA (N64) teamsite.

(9) Oversee and reinforce DON DIACAP handbook requirements and the certification and accreditation of all CNIC systems with coordination from the region and site Information Assurance Managers.

d. Region and Site IAMs shall:

(1) Take operational direction from the HQ IAPM.

(2) Act as subject matter expert on matters related to Information Assurance.

(3) Perform the duties of the role as defined in the CNIC Information Assurance Workforce Improvement Program Manual. The manual is available on the G2 IA (N64) teamsite.

(4) Reinforce the tenets of the CNIC IA program within his/her designated area of responsibility.