



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5239.3

BUPERS-07

17 OCT 2011

BUPERS INSTRUCTION 5239.3

From: Chief of Naval Personnel

Subj: INFORMATION ASSURANCE INTERNAL AUDIT PROGRAM

- Ref:
- (a) SECNAVINST 5239.3B
 - (b) Information Assurance and Security Roadmap of 29 Feb 2008 (NOTAL)
 - (c) DoD Instruction 8510.1, DoD Information Assurance Certifications and Accreditation Process (DIACAP) of 28 Nov 2007
 - (d) Federal Information System Management Act (FISMA) of 2002
 - (e) DoD Directive 8530.1, Computer Network Defense (CND) of 8 Jan 2001
 - (f) DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM) of 13 Aug 2004
 - (g) CJCSI 5239.19, Information Assurance (IA) and Network Defense of Aug 2007
 - (h) Privacy Act of 1974
 - (i) SECNAVINST 5239.19
 - (j) DoD 8570.01-M, Information Assurance Workforce Improvement Program of Apr 2010
 - (k) SECNAV M-5239.1, Department of Navy (DON) Information Assurance Program of Nov 2005
 - (l) CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities of 9 Jul 2008
 - (m) Command Cyber Readiness Inspection (CCRI) Coordination Instruction of 22 Feb 2010
 - (n) Cyber Security Inspection (CSI) Coordination Instruction of 20 Apr 2011
 - (o) OPNAVINST 5239.1C
 - (p) SECNAVINST 5239.1

- Encl:
- (1) Information Assurance Manager Blue Team Preparation Guide
 - (2) Commander, Commanding Officer, or GS Equivalent Blue Team Preparation Guide

1. Purpose. To establish Bureau of Naval Personnel (BUPERS) policy to set forth the authority, mission, and functions of the

17 OCT 2011

information assurance internal audit program as directed by reference (a). This audit program is intended to ensure continuous improvement of the BUPERS information assurance (IA) posture to facilitate the highest level of information and information system confidentiality, integrity, availability, authenticity, and non-repudiation.

2. Background. References (a) through (p) establish audit areas of interest and details specific responsibilities for the BUPERS Command Information Officer (CIO) (BUPERS-07), the Command Information Assurance Manager (IAM), Blue Teams, and subordinate commands. The Blue Team is an internal audit team for Navy information technology (IT) infrastructure and will assist the BUPERS CIO in identifying potential weaknesses in the computing environment. The BUPERS Blue Team will work with subordinate commands during the pre-audit phase, audit phase, and post-audit phase to resolve any outstanding findings. These findings will give the BUPERS CIO and commanders, commanding officers (COs) or GS equivalent the capability to effectively allocate resources for the remediation of vulnerabilities.

3. Applicability. All BUPERS commands and their information systems are subject to a Blue Team audit.

4. Action. The BUPERS Blue Team will conduct regularly scheduled audits of subordinate commands. Commands will receive a minimum of a 60-day advance notice of a regularly scheduled visit and a minimum of a 5-day advance notice of a spot check. Notification will be provided by the receipt of a Blue Team Coordination Package via e-mail. This package will contain enclosures (1) and (2) as well as other documentation that define pre-assessment, assessment, and post-assessment activities. The audit type and breadth will be determined by the BUPERS CIO and documented in enclosure (1). Audits may include all or part of the following areas:

- a. Validation of certification and accreditation per references (c) and (d);
- b. Evaluation of enclave and network security per reference (e);
- c. Verification of Security Technical Implementation Guide (STIG) implementation per reference (e);

17 OCT 2011

- d. Verification of adherence to Unclassified Trusted Network Protection Policy per reference (f).
- e. Performance of network-based vulnerability scans for IA vulnerability management compliance and assessment of compliance with Department Defense (DoD) IA policies per reference (g);
- f. Verification that personally identifiable information (PII) required protection is in place per reference (h);
- g. Audit of the incident handling process per reference (i);
- h. Audit of the information assurance workforce (IAWF) per reference (j);
- i. Audit of the overall IA program per reference (k); and
- j. Audit of the applicable BUPERS Defense Information Systems Network components per reference (l).

5. Responsibilities

a. The BUPERS CIO shall

- (1) Ensure commitment at all levels to support the Blue Team mission to proactively identify and remediate vulnerabilities in a timely manner, while providing an active and forward looking defense of Navy information systems;
- (2) Provide oversight for the Blue Team;
- (3) Provide resources to support the Blue Team audit function;
- (4) Enforce all IA compliance; and
- (5) Conduct a post visit out-brief with the commander, CO or GS equivalent and provide written report of findings to the Deputy Chief of Naval Personnel within 15 days of the audit conclusion.

17 OCT 2011

b. Commanders, COs or GS Equivalent shall

(1) Support the Blue Team mission to proactively identify and remediate vulnerabilities, while providing an active and forward looking defense of Navy information systems;

(2) Provide resources to support the audit. If the audit is a requested assist visit, provide travel funding (if required) and any funding related to the remediation phase; and

(3) Review and sign enclosure (2).

c. Command IAM shall

(1) Support the Blue Team mission to proactively identify and remediate threats, while providing an active and forward looking defense of Navy information systems;

(2) Review and sign enclosure (2);

(3) Ensure compliance with the selected inspection items in enclosure (2);

(4) Adhere to deadlines outlined in the Blue Team coordination package; and

(5) Participate in post visit out-briefs.

d. Blue Team shall

(1) Provide Blue Team coordination package with all the pre-audit documentation to the command for review and completion prior to the Blue Team visit. Commands will receive a minimum of a 60-day advance notice of a regularly scheduled visit and a minimum of a 5-day advance notice of a spot check. The selected inspection items will be documented per enclosure (2);

(2) Provide a pre-audit brief to the command and leadership prior to auditing any IT system;

(3) Perform predetermined tasks as outlined in the Blue Team coordination package during the audit;

17 OCT 2011

- (4) Provide a post-audit brief with the initial findings of the audit to the command and BUPERS CIO;
 - (5) Develop and provide the command, BUPERS CIO, and BUPERS IAM with a final audit report; and
 - (6) Provide IT-related training and assistance to BUPERS commands upon request.
6. Point of Contact. BUPERS, Information Management Office, (BUPERS-073); all correspondence routed to e-mail address BUPERS_IA_TEAM@navy.mil.
 7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy (SECNAV) Manual M-5210.1 of November 2007.
 8. Reports. Reporting requirements contained in this instruction are exempt from reports control per SECNAV Manual M-5214.1 of December 2005



D. P. QUINN
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
<http://www.npc.navy.mil>

17 OCT 2011

INFORMATION ASSURANCE MANAGER BLUE TEAM PREPARATION GUIDE

Summary: The Command IAM shall conduct a Non-Classified Internet Protocol Routing Network (NIPRNET) self assessment provided by the BUPERS Blue Team pertaining to the selected area(s) of inspection. The completion of self assessments will also meet the requirements for the Defense Information Systems Agency (DISA) Command Cyber Readiness Inspection (CCRI) and Naval Network Warfare Command (NETWARCOM) Cyber Security Inspection Certification Program (CSICP).

Blue Team Background: Blue Team is an assessment methodology that expands upon the original NIPRNET Compliance Validations as mandated in references (l) and (p). The Blue Team provides an assessment of network security compliance with DoD IA policies and configuration requirements.

Requirements: The self assessment must be aligned with the Blue Team assessment components as documented in the IAM Blue Team Preparation Guide, and all results shall be forwarded to the Blue Team lead. This effort will allow significant vulnerabilities to be addressed prior to the Blue Team assessment, and it will create a one-to-one relationship between the results of both assessments.

Audit Items: (The BUPERS CIO will select the assessment components from the list below)

- Network Infrastructure
- Domain Name System (DNS) Configuration
- DNS Operating Systems-Windows
- DNS Operating Systems-UNIX
- Internal Vulnerability Scan
- Wireless Security
- Enclave Review
- Host Based Security System (HBSS) Review
- Traditional/Physical Security
- Demilitarized Zone (Embedded and Subscribers)
- IAWF Improvement Plan
- Access Management
- PII Protection
- STIG Implementation

17 OCT 2011

The Information Assurance Manager's signature below indicates the receipt and review of the Blue Team Coordination Package and an acknowledgment of the Command IAM's responsibility to support the audit and to comply with the BUPERS CIO vulnerability remediation plan.

Command Information Assurance Manager Signature

Date

**COMMANDER/COMMANDING OFFICER/GS EQUIVALENT
BLUE TEAM PREPARATION GUIDE**

Summary: Commanders, Cos or GS equivalent shall direct the completion of a Non-Classified Internet Protocol Routing Network (NIPRNET) self assessment provided by the BUPERS Blue Team pertaining to the selected area(s) of inspection. The completion of self assessments will also meet the requirements for the Defense Information Systems Agency (DISA) Command Cyber Readiness Inspection (CCRI) and Naval Network Warfare Command (NETWARCOM) Cyber Security Inspection Certification Program (CSICP).

Blue Team Background: Blue Team is an assessment methodology that expands upon the original NIPRNET Compliance Validations as mandated in references (l) and (p). The Blue Team provides an assessment of network security compliance with DoD IA policies and configuration requirements.

Requirements: The self assessment must be aligned with the Blue Team assessment components as documented in enclosure (2), and all results shall be forwarded to the Blue Team lead. This effort will allow significant vulnerabilities to be addressed prior to the Blue Team assessment, and it will create a one-to-one relationship between the results of both assessments.

The signature below indicates the receipt and review of the Blue Team Coordination package and an acknowledgement of the command's responsibility to support the audit and to comply with the BUPERS CIO vulnerability remediation plan.

Commander/Commanding Officer/GS Equivalent Signature

Date