



DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 2620.1
BUMED-M09B15
JUL 14 2015

BUMED INSTRUCTION 2620.1

From: Chief, Bureau of Medicine and Surgery

Subj: INFORMATION TECHNOLOGY INTERNAL AUDIT AND REVIEW INSTRUCTION

Ref: (a) BUMEDINST 5200.15
(b) National Institute of Standards and Technology
(NIST) Special Publication (SP) 800-53A, Revision 4
(c) Government Accountability Office (GAO) Federal
Information System Controls Audit Manual (FISCAM)

1. Purpose. To establish guidance and procedures to conduct Information Assurance (IA) assessment that evaluates existing policies, processes, and Cyber Security controls per references (a) through (c).

2. Background. To ensure the integrity, confidentiality, and availability of Bureau of Medicine and Surgery (BUMED) Headquarters (HQ) information as well as to protect and minimize exposure from advanced persistent threat, an assessment needs to be performed. Such assessment will help in determining the validity of controls contained in the security plans, policies, processes, and the corrective actions that need to be accomplished to correct the weakness or deficiencies.

3. Policy. A semi-annual review must be conducted, as directed by Information Systems Security Manager (ISSM), to ensure existing policies, procedures, and security controls are applied and consistent to fully support organizational goals and uninterrupted operations.

4. Responsibilities

a. BUMED HQ ISSM:

(1) Ensure the semi-annual audit is conducted using an approved BUMED and report any anomalies to the appropriate subject matter expert.

(2) Validate all standard operating procedures (SOPs) are accurate and relevant.

JUL 14 2015

(3) Review the assessment/audit report.

(4) Facilitate a cost-effective approach to correcting weaknesses or deficiencies consistent with BUMED mission needs.

b. Information Technology and Communication Services (ITACS) Personnel shall:

(1) With direction from ISSM, perform some self-assessment to evaluate the security of BUMED network and systems in compliance with Department of Defense directives and Department of the Navy policies.

(2) Create SOPs for all internal processes and operations.

(3) Advise BUMED ISSM of any security deficiencies that will hinder BUMED mission along with recommendation to remediate the deficiencies.

(4) With the concurrence of the ISSM, apply corrective measures to mitigate the findings.

5. Action. BUMED ISSM will ensure all personnel within ITACS are aware of the contents of this instruction.

6. Records. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

7. Report. The reporting requirements contained in this instruction are exempt from reports control per SECNAV M-5314.1 of Dec 2005, Part IV, paragraph 7k.

8. Form. BUMED 2620/1 (07-2015), Information Technology Internal Audit, is available at:
<http://www.med.navy.mil/directives/Pages/BUMEDForms.aspx>


P. B. COE
Chief of Staff

Distribution is electronic only via the Navy Medicine Web site at:
<http://www.med.navy.mil/directives/Pages/BUMEDHQInstructions.aspx>