

~~FOR OFFICIAL USE ONLY~~

Naval Audit Service



Audit Report



Followup on Controls over Navy Marine Corps Intranet Contractors and Subcontractors Accessing Department of the Navy Information

~~Do not release outside the Department of the Navy
or post on non-NAVAUDSVC Web sites
without prior approval of the Auditor General of the Navy~~

N2014-0030
9 July 2014

Obtaining Additional Copies

To obtain additional copies of this report,
please use the following contact information:

Phone: (202) 433-5757
Fax: (202) 433-5921
E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-
5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits,
please use the following contact information:

Phone: (202) 433-5840 (DSN 288)
Fax: (202) 433-5921
E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005



DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
N2014-012
9 July 2014

**MEMORANDUM FOR PROGRAM EXECUTIVE OFFICER-ENTERPRISE INFORMATION
SYSTEMS**

**Subj: FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET
CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT
OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

- Ref:
- (a) Naval Audit Service Audit report N2011-0038 dated 26 May 11; Subj: "Controls over Navy Marine Corps Intranet Contractors and Subcontractors Accessing Department of the Navy Information"
 - (b) Secretary of the Navy Memo of 11 Oct 13; Subj: "Tasking Memorandum for Approved Recommendations from Rapid Reviews"
 - (c) Naval Audit Service memo 2014-012 of 2 Dec 13
 - (d) Naval Audit Service Terms of Reference of 15 Nov 13; Subj: "Terms of Reference for a follow-on review of security clearance controls over contractor and subcontractors under the Continuity of Service Contract"
 - (e) U.S. Navy Judge Advocate General's Manual Investigation of 8 Nov 13
 - (f) Naval Audit Service Memo of 3 Feb 2014; Subj: Preliminary results for the followup review of security clearance controls over contractor and subcontractors under the Continuity of Service Contract
 - (g) Secretary of the Navy Instruction 7510.7F, "Department of the Navy Internal Audit"

1. Introduction.

a. In response to reference (b), regarding a followup review of the Navy's Navy-Marine Corps Intranet (NMCI) Continuity of Services Contract (CoSC), the Naval Audit Service (NAVAUDSVC) performed a review as agreed in reference (d) and announced in reference (c) to verify that Program Executive Office, Enterprise Information Systems' (PEO EIS') plan of action properly addresses the security clearance controls and oversight deficiencies identified in references (a) and (e). This report provide the results of our review regarding PEO EIS' actions addressing security controls and oversight deficiencies as identified in our prior audit in reference (a).

Subj: **FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

b. We found that, as of 31 January 2014, although PEO EIS and the Naval Enterprise Networks Program Office (PMW 205) had taken some actions to address the recommendation in NAVAUDSVC final report N2011-0038, the intent of the recommendation had not been met. Specifically, they had not developed an oversight plan detailing how the program office would oversee contractor and subcontractor security clearance controls. They also did not have a plan of actions with milestones for developing and implementing an oversight plan to ensure that PEO EIS and PMW 205 properly address the security clearance controls and oversight deficiencies identified in reference (a). This occurred because PMW 205 initially stated on 26 May 2011 their office does not have the capability to oversee personnel not directly assigned to their office. In addition, they stated on 30 June 2011 they would task other organizations, including Defense Contract Management Agency, Defense Security Service, and the NMCI prime contractor with establishing the personnel security surveillance program. Also, program office personnel believed that the list of actions identified in the PEO EIS weekly updates sufficiently met the intent of the recommendation. See Paragraph 6, Audit Results, for details of the recommendation.

c. PEO EIS and PMW 205 officials agreed with our conclusions during a 31 January 2014 meeting with the audit team. The officials said they plan to establish and implement a plan of action with milestones for developing and implementing an oversight plan that details how the program office would oversee contractor and subcontractor security processes and controls, including security clearance controls. On 11 February 2014, we met with the Principal Civilian Deputy Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN RDA), at his request, along with the Program Executive Officer for Enterprise Information Systems to discuss NAVAUDSVC's preliminary results memorandum of 3 February 2014. During the meeting, PEO EIS stated they would have an oversight plan completed by 31 March 2014. See Paragraph 6 for our results.

2. Reason for Audit. A shooting incident at the Washington Navy Yard on 16 September 2013 was found to be related to the NMCI Continuity of Services Contract. As a result of this incident, the Secretary of the Navy (SECNAV) requested NAVAUDSVC (reference (b)) to perform a followup review of security clearance controls over the contractor and subcontractors working under the NMCI CoSC. In response to the SECNAV tasking, we performed a followup review, as agreed in reference (c). The audit objective was to verify that PEO EIS's plan of action properly addresses the security clearance controls and oversight deficiencies identified in our previous audit N2011-0038.

3. Background. On 26 May 2011, Naval Audit Service (NAVAUDSVC) issued audit report N2011-0038 (reference (a)), which found that the Navy Marine Corps Intranet (NMCI) Program Office¹ had not established an oversight mechanism to perform periodic inspections to ensure that

¹ Naval Enterprise Networks Program Office (PMW 205), formerly called the NMCI program office, currently has under their portfolio the Navy Marine Corps Intranet program as well as the Next Generation Enterprise Network (NGEN). The Program Executive Office for Enterprise Information Systems (PEO EIS) oversees these enterprise-wide information technology programs.

Subj: **FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

the NMCI prime contractor and its subcontractors were complying with Department of the Navy (DON) security and information technology access policies for contractor and subcontractor employees. NAVAUDSVC recommended that PEO EIS develop and implement an oversight plan that would alert the program office if contractor/subcontractor personnel who require security clearance or information technology-level access background checks are not receiving them in accordance with DON policies. On 30 June 2011, PEO EIS proposed a series of planned actions to address the identified weakness. However, the actions were never implemented.

b. Due to actions that were being taken following the Navy Yard shooting that will address the recommendation and resolve the deficiencies cited in N2011-0038, we did not perform an audit of the NMCI CoSC to review and test internal controls and oversight over security clearances, as initially agreed in reference (d). Therefore, we are not making recommendations in this report.

4. Communications with Management. We met with officials from PEO EIS and the Naval Enterprise Networks Program Office (PMW 205) on 28 March 2014 to discuss the status of actions being taken to develop and implement an oversight plan to address the recommendation in report N2011-0038. On 12 and 25 March 2014, we met with various officials from Department of Defense and DON organizations, including PMW 205, to provide feedback regarding the program office's draft of a Contract Security Oversight Program. We also met with PEO EIS and PMW 205 personnel on 31 January 2014 to brief them on our preliminary followup review results.

5. Scope and Methodology.

a. We conducted numerous interviews with process owners and management personnel between 19 December 2013 and 16 January 2014 to obtain an understanding of corrective actions planned and taken to address the recommendation in N2011-0038.

b. We obtained and reviewed PEO EIS and PMW 205 Corrective Action Progress Details relating to actions being taken. We examined underlying documentation and supporting information to determine whether the actions being taken sufficiently addressed the recommendation in N2011-0038. We also discussed the security clearance process with key personnel including PEO EIS, PMW 205, and contractor personnel to obtain an understanding of changes that have taken place as a result of corrective actions to address the tasking by the Secretary of the Navy (reference (b)).

c. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Subj: **FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

6. Pertinent Guidance.

a. FAR 46.401 (a) states government contract quality assurance shall be performed at such times as may be necessary to determine that the supplies or services conform to contract requirements. The plans should specify work requiring surveillance; and method of surveillance.

b. DoD 5220.22-M, “National Industrial Security Program,” states that contractors are required to report certain events that have an impact on the status of an employee's personnel security clearance (PCL), that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised. Also, employees, before being granted access to classified information, shall receive an initial security briefing that provides threat awareness briefing, defensive security briefing, overview of the security classification system, employee reporting obligations and requirements and security procedures and duties applicable to the employee's job. Also, some form of security education and training needs to be done at least annually, and refresher training to reinforce information provided.

c. SECNAV M5510.30, “Personnel Security Program,” states that a personnel security determination requires an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. It also requires indoctrination and orientation training on National Security implication of their duties, and annual refresher.

7. Audit Results.

a. In audit report N2011-0038, we recommended that PEO EIS “develop and implement an oversight plan that would alert the Navy Marine Corps Intranet Program Management Office if contractor/subcontractor personnel who require security clearances or information technology-level access background checks are not receiving them in accordance with Department of the Navy policies.”

b. In response to our followup audit work, PMW 205 developed and planned to implement an oversight plan, manual, and instruction, effective 4 April 2014. We also determined during this audit following the 16 September 2013 Navy Yard shooting, PEO EIS and PMW 205 had completed the following actions:

- Conducted a security stand down with participation of Government and contractor personnel providing an overview of the findings and the recommendation in our report N2011-0038, and communicating to attendees the new efforts they will be taking to improve controls over contractor security clearances;
- Created a Security Assistant Program Manager (SAPM) position and designated an acting SAPM;

Subj: **FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

- Mapped out processes to gain an understanding of Security Clearance and Common Access Card (CAC) issuance processes;
 - Identified preliminarily improvements from mapping security clearance and CAC issuance processes;
 - Began developing and disseminating training covering PMW 205 CoSC Security improvement and continuous evaluation program to the security team, Administrative Contracting Officer (ACO), and Contracting Technical Representatives; and
 - Appointed an ACO, who will be conducting reviews of contractor documentation and processes to ascertain compliance with Personnel Security Program and National Industrial Security Program requirements according to activity personnel.
- b. Based on our review of PMW 205's Contract Security Oversight Program Manual and related Instruction, and the Naval Enterprise Network Contract Security Surveillance Plan of Action of 31 March 2014 for the CoSC and Next Generation Enterprise Network Contract, we feel that actions taken to address security clearance controls and oversight deficiencies meet the intent of the recommendation in our prior audit report N2011-0038.

8. Conclusion. PEO EIS and PMW 205 have made progress in addressing the security and oversight deficiencies identified in our report N2011-0038. However, until these controls are fully implemented and sufficient time has passed for the corrective actions to fully take effect, it would be premature for us to perform an audit of security clearance controls over the contractor and subcontractors on the NMCI CoSC and the subsequent Next Generation Enterprise Network Contract. Therefore, we are making no recommendations in this report.

9. Federal Managers Financial Integrity Act. The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal Agency head to annually certify the effectiveness of the agency's internal and accounting system controls. In our opinion, the conditions noted in this report do not warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

10. Other Information.

a. Any requests for this report under the Freedom of Information act must be approved by the Auditor General of the Navy as required by reference (b). This report is also subject to follow-up in accordance with reference (b). If you have any questions, or wish to provide correspondence or schedule a closing conference, please contact Audit Director XXXXXXXXXXXXXXXX,

FOIA (b)(6)

Subj: **FOLLOWUP ON CONTROLS OVER NAVY MARINE CORPS INTRANET CONTRACTOR AND SUBCONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION (AUDIT REPORT N2014-0030)**

XXXXXXXXXXXXXXXXXXXXXXXXX or XXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX.

b. We appreciate the cooperation and courtesies extended to our auditors.



FOIA (b)(6)

XXXXXXXXXXXXXXXXXXXXX
Assistant Auditor General
Research, Development, Acquisition, and Logistics
Audits

Copy to:
UNSECNAV
DCMO
OGC
JAG, Navy
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N40, N41)
CMC (DMCS, APMC)
DON CIO
NAVINGEN (NAVIG-14)
PMW-205
AFAA/DO

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies

of this report