

Naval Audit Service



Audit Report



Contractors Accessing Department of the Navy Information on Non-Navy Marine Corps Intranet Networks

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

*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*

N2011-0056

7 September 2011

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

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

<http://secnavportal.donhq.navy.mil/nauditservices>



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

7510
N2010-NFA000-0068
7 Sep 2011

MEMORANDUM FOR DEPARTMENT OF NAVY CHIEF INFORMATION OFFICER
COMMANDER, NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER
COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS CENTER-ATLANTIC
COMMANDER, OFFICE OF NAVAL INTELLIGENCE

Subj: **CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS (AUDIT REPORT N2011-0056)**

Ref: (a) NAVAUDSVC memo N2010-NFA000-0068, dated 6 Apr 2010
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

1. The report provides the results of the subject audit announced in reference (a). Section A of the report provides our finding and recommendations, summarized management responses, and our comments on the responses. Section B provides the status of recommendations. The full text of management responses is included in the Appendices.

Command	Finding No.	Recommendation No.
Department of the Navy Chief Information Officer	1	1
Commander, Naval Education and Training Professional Development and Technology Center	1	2-4
Commander, Space and Naval Warfare Systems Center-Atlantic	1	5-6
Commander, Office of Naval Intelligence	1	7-8

2. Actions planned by Department of the Navy Chief Information Officer meet the intent of Recommendation 1. Actions planned by Commander, Naval Education and Training Professional Development and Technology Center meet the intent of Recommendations 3 and 4. Actions planned by Space and Naval Warfare Systems Center-Atlantic meet the

Table of Contents

SECTION A: FINDING, RECOMMENDATIONS, AND CORRECTIVE ACTIONS	1
Finding: Authorization for Access	1
Synopsis.....	1
Reason for Audit.....	1
Noteworthy Accomplishment.....	2
Pertinent Guidance	2
Audit Results	4
Naval Education and Training Professional Development and Technology Center.....	5
Space and Naval Warfare Systems Center-Atlantic.....	7
Office of Naval Intelligence.....	8
Conclusion.....	9
Recommendations and Corrective Actions	10
SECTION B: STATUS OF RECOMMENDATIONS	15
EXHIBIT A: BACKGROUND	17
EXHIBIT B: SYSTEM AUTHORIZATION ACCESS REQUEST-NAVY	20
EXHIBIT C: SCOPE AND METHODOLOGY.....	24
Federal Manager’s Financial Integrity Act.....	27
EXHIBIT D: ACTIVITIES VISITED AND/OR CONTACTED	28
APPENDIX 1: MANAGEMENT RESPONSE FROM DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.....	29
APPENDIX 2: MANAGEMENT RESPONSE FROM COMMANDING OFFICER, NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER	34
APPENDIX 3: MANAGEMENT RESPONSE FROM COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND	41
APPENDIX 4: MANAGEMENT RESPONSE FROM COMMANDER, OFFICE OF NAVAL INTELLIGENCE.....	44

Section A:

Finding, Recommendations, and Corrective Actions

Finding: Authorization for Access

Synopsis

The Department of the Navy (DON) Chief Information Officer needs to improve internal controls over the authorization process for contract employees and subcontract employees to access non-Navy Marine Corps Intranet networks. At three Navy commands visited, we audited 133 contract employees who accessed non-Navy Marine Corps Intranet networks during the period 1 October 2008 to 31 March 2010. We found 122 contract employees had both a background investigation and a proper level of security clearance; 6 contract employees had accurately completed System Authorization Access Request – Navy/access request forms; and 84 contract employees had completed training to access the network as required by Department of Defense (DoD) guidance. However, 11 contract employees did not have documented background investigations or security clearances prior to accessing the network; 127 had incomplete, inaccurate, or unaccounted for access request forms; and 44 contract employees had not completed the required initial training. This occurred because personnel: (1) were not verifying evidence of contract employee’s identity/security clearances and completion of access request forms prior to granting network access; and (2) were not documenting employee’s initial training. Failure to properly authorize access to DON non-Navy Marine Corps Intranet networks and provide initial training, increases the risk for theft of DON-sensitive and personal information.

Reason for Audit

The audit objectives were to verify that: (1) contractor and subcontractor personnel were properly authorized, and received appropriate training, to access information on non-Navy Marine Corps Intranet networks, and (2) remedial actions were taken if information security was breached.

This audit was requested by the DON Chief Information Officer. The request was in response to an incident involving a subcontractor’s employee who was not properly screened before providing service to the Navy. The unknown nature of internal controls and magnitude of risks in the contractor arena raise serious questions about contractor access, and safeguarding of DON information and personally identifiable information.

Noteworthy Accomplishment

Prior to the audit, the Naval Education and Training Professional Development and Technology Center initiated an internal review of all access request forms for contract employees with command access. This was prior to our recommendation for periodic inspection of the forms. The command modified the check-in/check-out and document review processes as a result of their review.

Pertinent Guidance

DoD 5200.2-R, “Personnel Security Program” January 1987 administrative reissuance incorporated through 23 February 1996, establishes policies and procedures to ensure that granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

- **Section C3.1.1** states that certain civilian positions within DoD entail duties of such a sensitive nature that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions.
- **Section C7.1.3.1** states that access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual’s suitability for such access. Rather they are decisions made by the commander that access is officially required.

DoD Instruction 8500.2, “Information Assurance Implementation” dated 6 February 2003 implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of DoD information systems and networks. Section 5.9.1 states that information assurance managers are to develop and maintain an organization- or DoD information system-level information assurance program that identifies information assurance processes and procedures. Section 5.9.2 states that information assurance managers are to ensure that information ownership responsibilities are established for each DoD information system, including access approvals. Section 5.10.1 requires all users have the requisite security clearances and supervisory need to know authorization, and are aware of the information assurance responsibilities before being granted access to DoD information systems.

DoD “Information Assurance Workforce Improvement Program” 8570.01-M, dated December 2005, provides guidance and procedures for the training, certification, and management of the DoD workforce conducting information assurance functions in

assigned duty positions. Section C6.2.2 states that to ensure understanding of the critical importance of information assurance, all individuals with access to DoD information technology systems are required to receive initial information assurance orientation before being granted access to the system, and annual information assurance awareness training to retain access.

Secretary of the Navy Instruction 5430.7Q, “Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy,” dated 17 August 2009, assigns Department-wide responsibilities for administration of the Department of the Navy. The Chief Information Officer serves as the Department’s principle advisor on information management, information technology, and information resource management matters, and is responsible for these matters within DON. The DON Chief Information Officer has oversight for the information management function within the Office of the Secretary of the Navy, Office of the Chief of Naval Operations, and Headquarters Marine Corps.

Secretary of the Navy Memorandum M-5510.30 “Department of the Navy Personnel Security Program,” dated June 2006, provides maximum uniformity and effectiveness in the application of Personnel Security Program policies throughout DON. Section 5-2 states that:

- The sensitivity- and information technology-level assigned will dictate the personnel security requirements; the greater the sensitivity, the greater the personnel security requirements; and
- Position designations will be at the highest level required by the incumbent’s specific duties. When the level of potential damage or privilege and other position characteristics appear to indicate differing levels of designation, the higher designation will always be used.

Section 9-20 states that the commanding officer’s duty to protect the command against the action of untrustworthy persons is paramount. The commanding officer has the prerogative of requesting trustworthiness through a National Agency Check or Facility Access National Agency Check to ensure the individuals who are permitted access to command persons, property, and facilities are trustworthy.

Commander Naval Network Warfare Command, Computer Tasking Order 08-05 Serial A, “Policy on Use of DoD Information Systems,” dated July 2008, directs the immediate implementation of the System Authorization Access Request-Navy form for all users requiring access to Navy information technology resources.

Audit Results

The DON Chief Information Officer needs to improve internal controls over its authorization process for contractors and subcontractors to access non-Navy Marine Corps Intranet networks. At three DON commands visited, we audited 133 (39 percent) of 337 contract employees who accessed 3 networks during the period 1 October 2008 to 31 March 2010. We found 122 contract employees had a proper level of security clearance; 6 contract employees had accurately completed System Authorization Access Request-Navy forms; and 84 contract employees had completed required training to access the network. However, 11 contract employees lacked a proper security clearance; 127 had incomplete, inaccurate, or unaccounted for access request forms; and 44 contract employees did not have the required training. This occurred because personnel: (1) were not verifying evidence of contract employees' identity/security clearances and completion of access request forms prior to granting network access, and (2) were not documenting employees' initial training. The effect of not following guidance for properly authorizing access to the networks increases the risk for theft of DON sensitive and personal information. The three commands were not aware of any breaches in security within the past 12 months. Details explaining our scope and methodology are in Exhibit C. The following chart shows command results.

	Sample of Contract Employees	No Security Clearance/ Background Investigation	Systems Authorization Access Request-Navy Form		Training Not Documented	
			No Forms	Forms Incomplete or Inaccurate	Information Assurance	Personally Identifiable Information
Naval Education and Training Professional Development and Technology Center	66	11	3	57	19	25*
Space and Naval Warfare Systems Center-Atlantic	1	0	0	1	0	N/A
Office of Naval Intelligence	66	0	27	39	19	N/A
Totals	133	11	30	97	38	25

* A total of 25 were missing some aspect of training: 19 were missing both information assurance and personally identifiable information training and six were missing only personally identifiable information training.

Figure 1: Command Results

Naval Education and Training Professional Development and Technology Center

We reviewed 66 (43 percent) of 153 contract employees granted access to one of the Naval Education and Training Professional Development and Technology Center's networks. The command has operational control and oversight over the geographically distributed network. As a result, the command relies on local area commands to authorize contract employees who access the network. However, Naval Education and Training Professional Development and Technology Center has final responsibility for the contract employees accessing the training network. The command followed a standard process for granting access to contract employees working on the training network. Every contract employee is required to complete a System Authorization Access Request-Navy form. This form identifies:

- The contract employee's Social Security Number (partial or full);
- Type of access requested;
- Completion of background investigation and security clearance level;
- Date initial information assurance training was completed;
- All appropriate signatures and consents (i.e., endorsement for access); and
- Justification for access.

According to the command's standard operating procedures, the information assurance manager is responsible for verifying the completion of training and required access forms. These procedures also state that each block/section of the access request form must be accurate and complete before the information assurance manager will accept the form and approve access to the network. Once the completion of the forms is verified, the information assurance manager submits an account creation request for each contract employee. The security manager verifies the type of security clearance for every contract employee, and whether a background investigation has been completed through the Joint Personnel Adjudication System. Once the background investigation has been verified, the security manager signs, dates, and completes the applicable section on the access request form. The information assurance manager then indicates that a contract employee is approved and/or verified for access by signing and dating the access request form. A contract employee is granted access to a network account only after completing the required access request form, information assurance training, and a Government employee has verified the completion of a background investigation through the Joint Personnel Adjudication System. We reviewed a total of 66 contract employees' security records through the Joint Personnel Adjudication System, access request forms, and training documentation.

Joint Personnel Adjudication System

DoD 5200.2R states persons in connection with the education and orientation of military personnel shall have been the subject of a favorably adjudicated National Agency Check prior to such assignment. We determined that 55 (83 percent) of 66 contract employees had the appropriate security clearance level and had undergone the correct adjudication. We found that 11 (17 percent) of 66 contract employees had access to the network, but had no record of a favorable adjudication/background investigation. This occurred because appropriate personnel did not verify information in the Joint Personnel Adjudication System. According to Secretary of the Navy M-5510.30, commanders are responsible for protecting the command against the actions of untrustworthy persons. With no evidence of adjudications/background investigations, the command cannot ensure these contract employees do not pose a threat to command security or otherwise endanger national security. Based on our findings, we projected that 26 (17 percent) of 153 contract employees had no records of favorable adjudications/background investigations (see Exhibit C).

Systems Authorization Access Request-Navy Form

We requested access request forms for 66 contract employees who had access to the network from 1 October 2008 through 31 March 2010. The forms, when validated by a DON official, serve as management control of access to DON networks. We received 63 (95 percent) of the 66 contract employees' forms. The command had no documentation for the remaining 3 (5 percent) contract employees. We projected that 7 (5 percent) of 153 contract employees' access request forms were missing (see Exhibit C). In addition, we found that 6 (9 percent) of 66 access request forms were properly processed as required by Commander Naval Network Warfare Command, Computer Tasking Order. However 57 (86 percent) forms were not. For example, the access request forms: (1) were missing security validations and designation of information technology access level; (2) had no signature of approval by the information assurance manager and/or security manager; or (3) had late signatures of approval. This happened due to personnel not documenting reviews, conducting late reviews, and not maintaining documentation. Based on our findings, we projected that 132 (86 percent) of 153 contract employees forms were not processed according to written policies and procedures (see Exhibit C). Without having adequate controls over the completion and retention of forms, the command cannot ensure contract employees are trustworthy and do not pose a threat to national security (see Exhibit B for a blank System Authorization Access Request-Navy form).

Training

The Naval Education and Training Professional Development and Technology Center's standard operating procedures state that any individual accessing a local network must

complete initial information assurance and personal identifiable information training. The information assurance manager is responsible for verifying contract employees' completion of initial training before access is granted.

We found that 36 (55 percent) of 66 contract employees completed required initial information assurance and personally identifiable information training. However, 25 (38 percent) of 66 contract employees were accessing the network without evidence of required initial training. Specifically, 6 (24 percent) of 25 contract employees were missing required initial personal identifiable information training, and 19 (76 percent) of 25 contract employees were missing both initial information assurance and personal identifiable information training before accessing the network. This occurred because contract employees were not taking the training and/or command personnel were not maintaining required documentation. Based on our findings, we projected that 58 (38 percent) of 153 contract employees did not complete required training prior to gaining access to the network (see Exhibit C). Without the proper security training the command cannot reasonably assure contract employees are knowledgeable regarding threat awareness and protection of sensitive information.

Space and Naval Warfare Systems Center-Atlantic

It is a business practice of Space and Naval Warfare Systems Center-Atlantic to require contractors to apply for a common access card and undergo a background investigation prior to requesting access to the command's networks. The background investigation is monitored by a trusted security agent throughout this process to ensure it has been completed prior to a contract employee receiving a common access card. A contract employee is granted access to a network account only after completing the required System Authorization Access Request-Navy form, information assurance training, and a Government employee has verified the completion of a background investigation through the Joint Personnel Adjudication System.

We selected the Naval Capital Region Research Development Technology and Education network for review, which has one contract employee performing administrative duties on the network. We reviewed the contract employee's security record through the Joint Personnel Adjudication System, access request form, and required training documentation. We found that the contract employee had the required security clearance and background investigation, and training was complete as required by Secretary of the Navy M-5510.30 and DoD Instruction 8570.1-M. However, the access request form was missing the information assurance manager signature of approval and there was no information technology-level designation by the security manager as required by local policies. Command personnel did not document approvals and did not review documentation. There is no reasonable assurance that the contract employee's background investigation was consistent with the level of network access (see Exhibit B for a blank System Authorization Access Request-Navy form).

Office of Naval Intelligence

We reviewed 66 (36 percent) of 183 contract employees who had access to one of the Office of Naval Intelligence networks. We found that personnel had no local guidance on the complete process of granting network access. We reviewed contract employees' security records through the Joint Personnel Adjudication System, System Authorization Access Request-Navy forms, and training documentation.

The command follows an unwritten procedure for granting contract employees access to any of their networks. We interviewed all Government personnel involved in the process for granting network access.

- Security is notified of the intent to bring contract personnel on board when the contracting office representative and/or the contract security officer submits a nomination package to Security.
- The command's security manager checks the Joint Adjudication Personnel System to verify the current security clearance/background investigation status on every contract employee.
- When the contract employee has the proper clearance then the information assurance officer creates a disabled account, and the security manager and/or contracting office representative schedules the contract employee for required indoctrination orientation.
- Once scheduled for indoctrination, the contract employee and sponsor are required to complete Part I of the access request form. The indoctrination process is a 2 day course that covers required specific security briefings and information assurance training.
- Upon completion of indoctrination, contract employees are granted specific security access. The information assurance manager's office and security officer complete the Systems Authorization Access Request-Navy form.
- Once granted specific security access, the contract employee's accounts are enabled.

Joint Personnel Adjudication System

The Office of Naval Intelligence requires specific security access and a Single Scope Background Investigation prior to gaining access to their network. We determined whether a contract employee had undergone the required investigation and whether the investigation had resulted in an eligible/ineligible determination for specific security access. All 66 contract employees had the specific security adjudication and background investigation records in the Joint Personnel Adjudication System.

Systems Authorization Access Request-Navy Form

We requested access request forms for 66 contract employees who had access to Office of Naval Intelligence Unclassified network from 1 October 2008 through 31 March 2010. The access request forms, when validated by a DON official, serve as a management control of access to DON networks. We received 39 (59 percent) of 66 contract employees' access request forms. The command had no documentation for the remaining 27 (41 percent) contract employees. However, when the command was notified of Commander Naval Network Warfare Command Computer Tasking Order 08-05, they immediately began contacting those 27 contract employee to complete the required access request form. We projected that 75 (41 percent) of 183 contract employees' access request forms were unaccounted for (see Exhibit C). Of the 39 access request forms received, none of them were properly completed and processed. For example, access request forms were missing designation of information technology access level, or had no signature of approval by the information assurance manager. This occurred because personnel were: (1) unaware of the access request form requirement; (2) not reviewing forms; and (3) not documenting approvals. Based on our findings, we projected that 108 (59 percent) of 183 contract employees' access request forms were not properly completed and processed (see Exhibit C) (see Exhibit B for a blank System Authorization Access Request-Navy form).

Training

We determined that on day 2 of the command indoctrination orientation, the information assurance manager briefed attendees on information assurance security. The command's training coordinator had attendees sign a muster sheet as proof of attendance. When the orientation is completed, the security manager sends an e-mail to account administration, listing attendees who completed command indoctrination. We verified that 47 (71 percent) of 66 contract employees had evidence of the initial information assurance training required by DoD Instruction 8570.01-M. However, 19 (29 percent) of 66 contract employees were accessing the network without any evidence of required initial information assurance training. This occurred because contract employees were not taking the training or command personnel were not maintaining required documentation. Based on our findings, we projected that 53 (29 percent) of 183 contract employees had no evidence of completed information assurance training prior to accessing the network (see Exhibit C).

Conclusion

Opportunities exist to improve DON's process of granting contractor and subcontractor personnel access to information on non-Navy Marine Corps Intranet networks. The need to properly authorize and receive appropriate training to access networks is a concern throughout DON. We found: (1) contract employees did not have documented

background investigations or security clearances prior to accessing the network; (2) system access forms were incomplete, inaccurate or missing; and (3) contract employees had not completed the required initial training. During our audit, the three commands visited were not aware of any breaches in security within the past 12 months. However, establishing effective policies and procedures will reduce DON's future risk of unauthorized access and disclosure of sensitive information.

Recommendations and Corrective Actions

The Department of the Navy Chief Information Officer provided a combined response for Recommendations 1 through 8, concurred with all recommendations, and all planned and completed corrective actions meet the intent of the recommendations.

Recommendations, summarized management responses, and Naval Audit Service comments on the responses are presented below. The complete text of management responses is in the Appendices.

We recommend that the Department of the Navy Chief Information Officer:

Recommendation 1. Provide oversight to ensure compliance with policies and procedures for granting contract employees' access to Department of the Navy networks as required by Secretary of the Navy Instruction 5239.3B.

Management response to Recommendation 1. Concur. Department of the Navy Chief Information Officer is coordinating with the Naval Inspector General to include this oversight in their command inspections. Department of the Navy Chief Information Officer is updating the Department of the Navy 2005 Effective Use Policy. Concurrently, the Navy is updating the System Authorization Access Request-Navy form. Estimated completion date is 31 December 2011.

Naval Audit Service comment on response to Recommendation 1. Department of the Navy Chief Information Officer actions planned to update Department of the Navy policy and Naval Inspector General command inspections, in conjunction with the Navy updating the System Authorization Access Request-Navy form, meets the intent of the recommendation.

We recommend that Commander, Naval Education and Training Professional Development and Technology Center:

Recommendation 2. Suspend network accounts for contract employees who have no record of security clearances/background investigations in the Joint Personnel Adjudication System until issues are resolved.

Management response to Recommendation 2. Concur. Naval Education and Training Professional Development and Technology Center has resolved 10 of the 11 instances in which there was no record of a favorable adjudication/background investigations for contract employees. In addition, the Center is taking action to conduct a review of all contract employees to verify that all have a background investigation or security clearance on file. Naval Education and Training Professional Development and Technology Center will suspend the account of any contract employee with no record of a favorable background investigation or security clearance. Estimated completion date is 31 August 2011.

Naval Audit Service comment on response to Recommendation 2. Actions taken and planned meet the intent of the recommendation. In subsequent communication, the Naval Education and Training Professional Development and Technology Center stated the contractor in question received a favorable adjudication/background investigation on 18 July 2011 and suspension is not needed and the action is considered complete.

Recommendation 3. Review System Authorization Access Request-Navy forms and training documentation for all contract employees for completeness.

Management response to Recommendation 3. Concur. Naval Education and Training Professional Development and Technology Center's Contracting Officer's Representative will develop and implement a process to perform periodic inspections of contractor System Authorization Access Request-Navy forms. Also, the Technical Assistance appointment letter has been revised to include "coordinating" the background/security and System Authorization Access Request-Navy information/requirements. Additionally, the Fiscal Year 2012 Task Order will incorporate these requirements. Estimated completion date is 31 December 2011.

Naval Audit Service comment on response to Recommendation 3. Actions taken and planned meet the intent of the recommendation.

Recommendation 4. Update the local instructions to include, but not limited to: (1) requiring proper completion System Authorization Access Request-Navy forms before granting system access; (2) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (3) specifying retention period for training documentation as required in the Department of the Navy Records Management Program.

Management response to Recommendation 4. Concur. Although individual (remote) sites will be held responsible to ensure that internal controls for system access requirements are in place, Naval Education and Training Professional Development and Technology Center agrees that final responsibility for the

contract employees belongs to the command. The Center's Contracting Officer's Representative will develop and/or revise local instructions/documents to ensure proper completion of System Authorization Access Request-Navy forms, perform quarterly inspections of these forms for contractors, and retention of training documentation. In addition, the Fiscal Year 2012 Task Order will incorporate these requirements. Estimated completion date is 31 December 2011.

Naval Audit Service comment on response to Recommendation 4. Actions planned meet the intent of the recommendation.

We recommend that Commander, Space and Naval Warfare Systems Center-Atlantic:

Recommendation 5. Review System Authorization Access Request-Navy documentation for all contract employees for completeness.

Management response to Recommendation 5. Concur. Space and Naval Warfare Systems Center-Atlantic is currently reviewing all contract employee System Authorization Access Request-Navy forms for completeness. Estimated completion date is 31 May 2012.

Naval Audit Service comment on response to Recommendation 5. Action planned meets the intent of the recommendation.

Recommendation 6. Update standard operating procedures to include a requirement for quarterly inspections of System Authorization Access Request-Navy documentation for all new contract employees.

Management response to Recommendation 6. Concur. Space and Naval Warfare Systems Center-Atlantic is updating its Standard Operating Procedures/Process to include and implement a quarterly review process comparing new contractors with information technology access to System Authorization Access Request-Navy forms on file. Update and initiation of the process will be completed. Estimated completion date is 31 May 2012.

Naval Audit Service comment on response to Recommendation 6. Action planned meets the intent of the recommendation.

Additional Comments: Naval Education and Training Professional Development and Technology Center concurred with the overall finding and provided explanations regarding the finding. Command stated information and documentation were available during the audit. After being unable to verify security clearances for 11 contractors, we contacted the command several times. Command personnel stated the audit team was provided the correct Social Security Numbers for all contractors. Results were unchanged after a second attempt to verify security clearances. Hence, we could not verify whether the contractor personnel had security clearances.

Commander Naval Network Warfare Command's Computer Tasking Order 08-05, as implemented in Naval Education and Training Command's "Standard Operating Procedure for Completing the End User Agreement," requires a fully completed System Authorization Access Request with timely approvals in order to gain access to a network. With missing information and late or no approvals, we determined forms were not properly processed. Command's review actions were taken after Naval Audit Service's review of the information and documentation.

We recommend that Commander, Office of Naval Intelligence:

Recommendation 7. Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.

Management response to Recommendation 7. Concur. Hopper Information Service Center is working in concert with the Office of Naval Intelligence Special Security Office to execute a 100-percent inventory of System Authorization Access Request-Navy forms and associated training documentation for all 451 contractors who currently have access to Office of Naval Intelligence Sensitive but Unclassified Internet Protocol Router Network. Estimated completion date is 8 July 2011.

Naval Audit Service comment on response to Recommendation 7. Action planned meets the intent of the recommendation. In subsequent communication, the Office of Naval Intelligence stated that the review of documentation for all contractors was completed on 8 July 2011 as planned, and the action is considered complete.

Recommendation 8. Establish written standard operating procedures to include, but not limited to: (1) identifying processes for granting network access; (2) requiring proper completion of System Authorization Access Request-Navy forms; (3) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (4) specifying retention period for training documentation as required in the Department of the Navy Records Management Program.

Management response to Recommendation 8. Concur. Hopper Information Service Center is working with the Office of Naval Intelligence claimancy to draft an Office of Naval Intelligence Instruction that formally codifies a System Authorization Access Request-Navy and broader user access management Standard Operating Procedure assembled in May 2011 by a command-wide tiger team. The Instruction is on-track for Commander, Office of Naval Intelligence approval and subsequent promulgation. Estimated completion date is 31 August 2011.

Naval Audit Service comment on response to Recommendation 8. Action planned meets the intent of the recommendation.

Section B:

Status of Recommendations

Recommendations							
Finding ¹	Rec. No.	Page No.	Subject	Status ²	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³
1	1	10	Provide oversight to ensure compliance with policies and procedures for granting contract employees' access to Department of the Navy networks as required by Secretary of the Navy Instruction 5239.3B.	O	Department of the Navy Chief Information Officer	12/31/11	
1	2	10	Suspend network accounts for contract employees who have no record of security clearances/background investigations in the Joint Personnel Adjudication System until issues are resolved.	C	Commander, Naval Education and Training Professional Development and Technology Center	7/18/11	
1	3	11	Review System Authorization Access Request-Navy forms and training documentation for all contract employees for completeness.	O	Commander, Naval Education and Training Professional Development and Technology Center	12/31/11	
1	4	11	Update the local instructions to include, but not limited to: (1) requiring proper completion System Authorization Access Request-Navy forms before granting system access; (2) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (3) specifying retention period for training documentation as required in the Department of the Navy Records Management Program.	O	Commander, Naval Education and Training Professional Development and Technology Center	12/31/11	
1	5	12	Review System Authorization Access Request-Navy documentation for all contract employees for completeness.	O	Commander, Space and Naval Warfare Systems Center-Atlantic	05/31/12	

¹ / + = Indicates repeat finding.

² / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.

³ If applicable.

Recommendations							
Finding ¹	Rec. No.	Page No.	Subject	Status ²	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³
1	6	12	Update standard operating procedures to include a requirement for quarterly inspections of System Authorization Access Request-Navy documentation for all new contract employees.	O	Commander, Space and Naval Warfare Systems Center-Atlantic	05/31/12	
1	7	13	Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.	C	Commander, Office of Naval Intelligence	7/08/11	
1	8	13	Establish written standard operating procedures to include, but not limited to: (1) identifying processes for granting network access; (2) requiring proper completion of System Authorization Access Request-Navy forms; (3) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (4) specifying retention period for training documentation as required in the Department of the Navy Records Management Program.	O	Commander, Office of Naval Intelligence	8/31/11	

Exhibit A:

Background

The unknown nature of internal controls and magnitude of risks in the contractor arena raise serious questions about contractor access, and safeguarding of Department of the Navy (DON) information. Furthermore, the DON Chief Information Officer requested a review of Non-Navy Marine Corps Intranet networks in response to an incident involving a subcontractor who did not properly screen an employee before placing that employee to provide service to the Navy. Therefore, we selected three commands to review the authorization of access for employed contractors and subcontractors providing information technology services.

Naval Education and Training Professional Development and Technology Center, which is an Echelon III command, has operational control and oversight over the NETC_N00076_TRANET_U (training) network. However, the Naval Education and Training Center, an Echelon II command, is the owning command of the training network. Both commands are located in Pensacola, FL. The Naval Education and Training Professional Development and Technology Center provides quality products and services to support and enhance education, training, career development, and personnel advancement. The training network is a distributed learning environment that offers education, training, and student management to Service members, providing the tools and opportunities, which enable life-long learning, and enhance professional and personal growth and development. It is a networked structure of bases, buildings, logical classrooms, and data centers that provide training and education courseware/learning content for shore based facilities, as well as locations available via the Non-Classified Internet Protocol Router Network. Recipients of this training and education content include the enlisted and officer communities for the Department of Defense (DoD), as well as civilians, contractors, retirees, and military dependants.

Space and Naval Warfare Systems Center-Atlantic, located in Charleston, SC, is the owning command of the SPAWAR_N65236_NCR RDT&E_U network. The main focus of this network is to provide information technology support to DoD and Federal Government agencies. This network is part of the core Space and Naval Warfare Systems Center-Atlantic Research, Development, Testing and Evaluation's capability, and is critical to the Command Control Communication Computer Intelligence Surveillance Reconnaissance system integration, testing, and evaluation. It supports the development of leading edge, advanced concept technology, and provides a seamless lab-to-lab and ship-to-shore computing and networking collaboration environment. The network is host to a variety of customer systems and projects that process information up to the classification of unclassified sensitive information.

Office of Naval Intelligence is the owner of the ONI_N00015_ONI UNCLASSIFIED_U network. Founded in 1882, the Office of Naval Intelligence is the longest continuously operating intelligence service in the nation. The command employs more than 3,000 highly qualified military, civilian, mobilized reservists, and contractor personnel at the modern National Maritime Intelligence facility in Washington, DC, and at other strategic locations around the world. They produce maritime intelligence on seaborne terrorism, weapons and technology proliferation, narcotics and smuggling activities that directly supports joint war fighters, the U.S. Navy, civil and national decisionmakers, and agencies. The Office of Naval Intelligence's unclassified network is a Non-Secure Internet Protocol Router Network. The network consists of three systems:

1. Windows, which primarily houses e-mail, shared folders, application services, and Web product dissemination;
2. The Universal Network Information Exchange, which primarily houses Office of Naval Intelligence databases, cross domain services, and Web applications; and
3. The Special Local Area Networks, which also operates through Windows and houses e-mail, shared folders, application services, and Web product dissemination for a more limited customer set.

The DON Application and Database Management System is a Web-enabled registry of information technology applications and systems and their associated data structures and data exchange formats. It supports DON in the reduction of legacy applications, and the development of standard applications, databases, and data elements. It also supports information technology interoperability, information assurance assessments, and the construction and maintenance of functional and enterprise architecture. As of 20 April 2010 DON had a total of 383 Non-Navy Marine Corps Intranet networks registered in the DON Application and Database Management System.

The Joint Personnel Adjudication System is the DoD personnel security migration system for:

- The virtual consolidation of the DoD Central Adjudication Facilities;
- Use by non-Special Compartmented Information security program managers and special security officers;
- Special Access Program managers; and
- DoD contractor security officers.

The Joint Personnel Adjudication System uses a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes. The Joint Personnel Adjudication System automates both core and central

adjudication facilities-unique functionality and provides “real-time” information regarding clearance, access, and investigative status to authorized DoD security personnel and other interfacing organizations, such as the Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, and Air Force Personnel Center.

Exhibit B:

System Authorization Access Request-Navy

FOR OFFICIAL USE ONLY

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)			
PRIVACY ACT STATEMENT			
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records will be maintained in paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.			
TYPE OF REQUEST			DATE (YYYYMMDD)
<input type="checkbox"/> Initial <input type="checkbox"/> Modification <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____			
SYSTEM NAME (i.e., NMC, IT21, OnaNET, etc.)		LOCATION (Physical Location of System)	
PART I (To be completed by Requester)			
1. NAME (Last, First, Middle Initial)		2. SOCIAL SECURITY NUMBER (LAST FOUR)	
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. PHONE (DSN and Commercial) DSN: COM:	
6. OFFICIAL E-MAIL ADDRESS	7. JOB TITLE AND GRADE/RANK		
8. OFFICIAL MAILING ADDRESS	9. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> Other	10. DESIGNATION OF PERSON <input type="checkbox"/> Military <input type="checkbox"/> Contractor <input type="checkbox"/> Civilian	
11. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) _____			
12. USER SIGNATURE		13. DATE (YYYYMMDD)	
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 17a).			
14. JUSTIFICATION FOR ACCESS Access to Government IT Systems are required to execute duties as assigned.			
15. TYPE OF ACCESS REQUIRED: <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
16. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify Category): _____ <input type="checkbox"/> OTHER: _____			
17. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		17a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date)	
18. SUPERVISOR'S NAME (Print Name)	18a. SUPERVISOR'S SIGNATURE	18b. DATE (YYYYMMDD)	
19. SUPERVISOR'S ORGANIZATION/DEPARTMENT	19a. SUPERVISOR'S E-MAIL ADDRESS	18b. PHONE NUMBER	
20. SIGNATURE OF INFORMATION OWNER/OPR	20a. PHONE NUMBER	20b. DATE (YYYYMMDD)	
21. SIGNATURE OF IAO OR APPOINTEE	22. ORGANIZATION/DEPARTMENT	23. PHONE NUMBER	24. DATE (YYYYMMDD)

25. NAME (Last, First, Middle Initial)	25a. SOCIAL SECURITY NUMBER (LAST FOUR)
<p>26. USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION</p> <p>By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:</p> <ul style="list-style-type: none"> - You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only. - You consent to the following conditions: <ul style="list-style-type: none"> o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations. o At any time, the U.S. Government may inspect and seize data stored on this information system. o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose. o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy. o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below: <ul style="list-style-type: none"> - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality. - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies. - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality. - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy. - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality. - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected. o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information. o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement. 	
27. USER SIGNATURE	28. DATE (YYYYMMDD)

29. NAME (Last, First, Middle Initial)		29a. SOCIAL SECURITY NUMBER (LAST FOUR)	
30. USER RESPONSIBILITIES I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall: <ul style="list-style-type: none"> - Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use. - Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information. - Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system. - Virus check all information, programs, and other files prior to uploading onto any Navy IT resource. - Report all security incidents immediately in accordance with local procedures and CJCSM 8510.01 (series) - Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized. I further understand that, when using Navy IT resources, I shall not: <ul style="list-style-type: none"> - Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO!, AOL, etc.) - Auto-forward official e-mail to a commercial e-mail account. - Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (CO or OIC). - Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource. - Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority. - Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority. - Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority. - Participate in or contribute to any activity resulting in a disruption or denial of service. - Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code. - Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service). 			
31. USER SIGNATURE		32. DATE	
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
33. TYPE OF INVESTIGATION		33a. DATE OF INVESTIGATION (YYYYMMDD)	
33b. CLEARANCE LEVEL		33c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL 1 <input type="checkbox"/> LEVEL 2 <input type="checkbox"/> LEVEL 3	
34. VERIFIED BY (Print name)	35. SECURITY MANAGER TELEPHONE NUMBER	36. SECURITY MANAGER SIGNATURE	37. DATE (YYYYMMDD)
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION			
38. TITLE	38a. SYSTEM	38b. ACCOUNT CODE	
	38c. DOMAIN		
	38d. SERVER		
	38e. APPLICATION		
	38f. DIRECTORIES		
	38g. FILES		
	38h. DATASETS		
39. DATE PROCESSED (YYYYMMDD)	39b. PROCESSED BY (Print name and sign)	39c. DATE (YYYYMMDD)	
40. DATE REVALIDATED (YYYYMMDD)	40a. REVALIDATED (Print name and sign)	40b. DATE (YYYYMMDD)	

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Social Security Number. The last four numbers in the social security number of the user.
- (3) Organization. The user's current organization (i.e., USS xx, DoD, and government agency or commercial firm).
- (4) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
- (5) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
- (6) Official E-mail Address. The user's official e-mail address.
- (7) Job Title/Grade/Rank. The civilian job title (i.e., Systems Analyst, YA-02, military rank (CAPT, United States Navy) or "CONT" if user is a contractor.
- (8) Official Mailing Address. The user's official mailing address.
- (9) Citizenship (U.S., Foreign National or Other).
- (10) Designation of Person (Military, Civilian, Contractor).
- (11) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (12) User's Signature. User must sign the OPNAV 5239/14 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (13) Date. The date the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (14) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (15) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters or settings.)
- (16) User Requires Access To. Place an "X" in the appropriate box. Specify category.
- (17) Verification of Need to Know. To verify that the user requires access as requested
- (17a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (18) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (18b) Date. Date supervisor signs the form.
- (19) Supervisor's Organization/Department. Supervisor's organization and department.
- (19a) E-mail Address. Supervisor's e-mail address.
- (19b) Phone Number. Supervisor's telephone number.
- (20) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
- (20a) Phone Number. Functional appointee telephone number.
- (20b) Date. The date the functional appointee signs the OPNAV 5239/14.

- (21) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.
- (22) Organization/Department. IAO's organization and department.
- (23) Phone Number. IAO's telephone number.
- (24) Date. The date IAO signs the OPNAV 5239/14.
- (25) Name. The last name, first name, and middle initial of the user.
- (25a) Social Security Number. The last four numbers in the user's social security number.
- (26) Standard Mandatory Notice and Consent Provision. This item is in accordance with DoD memo dtd May 9, 2008 (Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement).
- (27) User Signature. User signs.
- (28) Date. Date signed.
- (29) Name. The last name, first, name and middle initial of the user.
- (29a) Social Security Number. The last four numbers in the social security number of the user.
- (30) User Responsibilities.
- (31) User Signature. Member signs.
- (32) Date. Date signed.

C. PART III: Certification of Background Investigation or Clearance.

- (33) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI or SSBI).
- (33a) Date of Investigation. Date of last investigation.
- (33b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
- (33c) IT Level Designation. The user's IT designation (Level I, Level II or Level III).
- (34) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
- (35) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
- (36) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
- (37) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the functional activity or the customer with approval from NAVNETWARCOM. This information will specifically identify the access required by the user (38 - 40b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If transmitted electronically, the email must be digitally signed and encrypted.

FILING: Retention of this form shall be in accordance with SECNAV M5210-1, Records Management Manual (Section 5230.2 applies).

Exhibit C:

Scope and Methodology

We judgmentally selected, through the Department of Navy (DON) Application and Database Management System, networks with a high, medium, and low number of devices connected to a network. The three networks selected were: (1) the Naval Education and Training Professional Development and Technology Center training network, Pensacola, FL; (2) the Space and Naval Warfare Systems Center-Atlantic Naval Capital Region Research Development Technology and Education network, Charleston, SC; and (3) the Office of Naval Intelligence unclassified network, Washington, DC. We reviewed the three commands' process of granting contract employees access to networks. This audit was performed between 18 May 2010 and 7 June 2011.

We did not test the reliability of data from the DON Application and Database Management System because such a test would have constituted a significant audit effort that was outside the scope of our audit work. We also did not test the reliability of data from the networks selected because such a test was outside the scope of our audit work.

There were no previous audits from the Naval Audit Service, Department of Defense Inspector General, or Government Accountability Office covering granting contract employees access to DON networks at the three commands visited.

We obtained and audited pertinent documentation, records, and reviewed policies and procedures used. We interviewed personnel involved in the process of granting contract employees access the DON networks. We assessed compliance with legal and regulatory requirements, and evaluated internal controls related to contract employees accessing networks. We reviewed applicable laws, policies, procedures, regulations, and directives relevant to the process of granting contract employees access to DON networks.

We reviewed 133 contractors and subcontracts (from a universe of 337) who had access to DON Non-Naval Marine Corps Intranet networks during 1 October 2008 through 31 March 2010.

- The Naval Education and Training Professional Development and Technology Center provided a universe of 153 contractors; from this universe we statistically selected 66 (43 percent) contractors for review;
- The Space and Naval Warfare Systems Center-Atlantic provided a universe of one contractor; and

- The Office of Naval Intelligence provided a universe of 183 contractors; from this universe we statistically selected 66 (36 percent) contractors for review.

The audit team interviewed command information assurance personnel to determine the process for granting a contractor access to a network specific to their business environment. At the three commands reviewed, the process for granting access was consistent:

- The contractor is to complete Part I of the access request form, sign the user agreement and responsibilities section of the System Authorization Access Request-Navy form, complete mandatory initial information assurance training, and record the date taken;
- The access request form, Part II, is to be completed by the Government sponsor of the contractor;
- After the completion of Parts I and II of the access request form, it is returned to the information assurance manager or information assurance officer. The information assurance manager or officer is responsible for verifying that training has been completed and the form is complete and accurate;
- The form is forwarded to the command security manager to complete and sign Part III, which validates date of background information and level of security clearance through the Joint Adjudication Personnel System; and
- Once all has been completed, the information assurance manager enables the contractor's account for access.

The audit team reviewed required System Authorization Access Request-Navy forms for:

- Accuracy of required information in accordance with Department of Defense (DoD), DON, and local policies; and
- Completeness of all required parts in accordance with DoD, DON, and local policies.

We also verified the completion of all required information assurance training, and verified contractors' background investigations and security clearances through the Joint Personnel Adjudication System.

Throughout the audit, we kept management officials from the Naval Education and Training Professional Development and Technology Center, Space and Naval Warfare Systems Center-Atlantic, and Office of Naval Intelligence informed of the conditions noted. We held opening conferences with the commands on 18 May, 21 June, and 15 September 2010, respectively. Preliminary audit results were briefed to Naval Education and Training Professional Development and Technology Center, Office of

Naval Intelligence, and Space and Naval Warfare Systems-Atlantic on 12 October 2010, 1 February 2011, and 9 February 2011, respectively.

Based on the sample results, the Naval Audit Service statistician calculated projections for the number of individuals missing training, the number of individuals with no evidence in the Joint Personnel Adjudication System who received a favorable adjudication, the number of individuals missing access request forms, and the number of individuals with incorrectly processed access request forms. The projections were carried out at the 90 percent confidence level, which means that there is a 10 percent risk that each interval does not encompass the true population value of interest. The results of these projections are in the following two tables.

The first row of the Naval Education and Training Professional Development and Technology Center table shows that it is likely that between 45 and 72 out of the 153 contractors were missing information assurance training. The point estimate, or best guess, for this projection was 58 contractors. The remaining estimates can be interpreted in a similar fashion.

Naval Education and Training Professional Development and Technology Center

	90% Lower Bound	Estimated Counts	90% Upper Bound
Missing Information Assurance Training	45	58	72
No Evidence of Favorable Adjudication in Joint Personnel Adjudication System	17	26	36
System Authorization Access Request-Navy Forms Missing	3	7	14
System Authorization Access Request-Navy Forms Incorrectly Processed	122	132	139
Universe Total = 153			

Office of Naval Intelligence

	90% Lower Bound	Estimated Counts	90% Upper Bound
Missing Information Assurance Training	40	53	68
No Evidence of Favorable Adjudication in Joint Personnel Adjudication System	0	0	6
System Authorization Access Request-Navy Forms Missing	60	75	91
System Authorization Access Request-Navy Forms Incorrectly Processed	92	108	123
Universe Total = 183			

The audit was conducted 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Federal Manager's 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. During this audit, we identified internal control weaknesses in the oversight and monitoring of contract personnel accessing DON non-Navy Marine Corps Intranet networks. In our professional judgment, the internal control weaknesses identified in this report may warrant reporting in the Auditor General's annual Federal Managers Financial Integrity Act memorandum identifying management control weaknesses to the Secretary of the Navy.

Exhibit D:

Activities Visited and/or Contacted

Commands Visited:

Commander, Naval Education and Training Professional Development and
Technology Center, Pensacola, FL

Space and Naval Warfare Systems Center-Atlantic, N. Charleston, SC

Commander, Office of Naval Intelligence, Washington, DC

Commands Contacted:

Department of the Navy Chief Information Officer, Arlington, VA

Space and Naval Warfare Systems Command, San Diego, CA

Space and Naval Warfare Systems Center-Pacific, San Diego, CA

Appendix 1:

Management Response from Department of the Navy Chief Information Officer



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000
~~FOR OFFICIAL USE ONLY~~

20 July 2011

MEMORANDUM FOR ASSISTANT AUDITOR GENERAL OF THE NAVY FOR
FINANCIAL MANAGEMENT AND COMPTROLLER AUDITS)

Subj: RESPONSE TO NAVAUDSVC DRAFT AUDIT REPORT N2010-0068, 7 JUN 2011,
CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION ON
NON-NAVY MARINE CORPS INTRANET NETWORKS

Ref: (a) Naval Audit Service ltr 7510 ser N2010-NFA0000-0068 of 7 Jun 2011

Encl: (1) DON CIO Response to NAVAUDSVC Draft Audit Report N2010-NFA000-0068

Reference (a) requires a response to subject audit. The audit contains eight recommendations for response by the Department of the Navy Chief Information Officer (DON CIO), Commander, Naval Education and Training Professional Development Technology Center, Space and Naval Warfare Systems Center-Atlantic, and Commander, Office of Naval Intelligence.

The DON CIO concurs with the audit findings and recommendations. In enclosure (1) we have provided the combined responses, as forwarded and approved by OPNAV N2/N6.

The DON CIO points of contact for this matter are [REDACTED]

[REDACTED]

[REDACTED]

Department of the Navy
Principal Deputy Chief Information Officer

Copy to:
OPNAV N2/N6 (Attn: N2/N6F15B)
NAVAUDGEN (Attn: [REDACTED])

~~FOR OFFICIAL USE ONLY~~

FOIA (b)6

FOIA (b)6

FOIA (b)6

The management response from DON CIO is not being treated as FOUO, therefore we are striking the FOR OFFICIAL USE ONLY markings on the management response. However, we are marking this page of the report FOUO because the management response contains personally identifiable information that is exemption from release under Freedom of Information Act Exemption (b)6.

~~FOR OFFICIAL USE ONLY~~

**DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER RESPONSE TO
NAVAL AUDIT SERVICE DRAFT AUDIT REPORT, N2010-NFA000-0068,
CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION ON
NON-NAVY MARINE CORPS INTRANET NETWORKS**

NAVAUDSVC Recommendation 1 for DON CIO Action:

Provide oversight to ensure compliance with policies and procedures for granting contract employees' access to Department of the Navy networks as required by Secretary of the Navy Instruction 5239.3B.

DON CIO Response:

Concur.

DON CIO is coordinating with the Naval Inspector General (NAVIG) to include this oversight in their command inspections. DON CIO is updating the DON 2005 Effective Use Policy. That policy memorandum is currently out for Flag/SES review. Language to address the concerns in the audit was inserted. Estimated completion on 1 September 2011.

Concurrently, the Navy is updating the System Authorization Access Request-Navy (SAAR-N) form, with estimated completion by 31 December 2011.

NAVAUDSVC Recommendation 2, 3, and 4 are addressed to the Commander Naval Education and Training Professional Development Technology Center (NETPDTC) for Action.

NAVAUDSVC Recommendation 2:

Suspend network accounts for contract employees who have no record of security clearances/background investigations in the Joint Personnel Adjudication System until issues are resolved.

NETPDTC Response:

Concur.

NETPDTC agrees that employees without record of security clearance or background investigation in the Joint Personnel Adjudication System (JPAS) should not have network accounts or access to the network. The following corrective actions have been taken:

(1) Upon receiving the preliminary audit results last fall, NETPDTC researched the 11 records reviewed in the audit and resolved 10 of the 11 instances of the issue of lack of record of a favorable adjudication/background investigation in November 2010. The record for one contract employee listed on the audit sampling has not yet been resolved for a favorable adjudication/background investigation. NETPDTC will suspend the network account for this contract employee by 31 August 2011 if the background investigation has not been resolved at the time. The suspension will continue until all issues are resolved.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

(2) The FY12 Statement of Work for the Computer Science Corporation (CSC) contract requires that all contract employees have a Common Access Card (CAC) before they are allowed on the network (if access is required to perform their job duties).

(3) After the initial audit finding, CSC reviewed all contract employee records for all 400+ contractors hired on the contract and made proper resolutions where necessary regarding 1) documentation of background investigations or security clearances; 2) proper completion of system access forms; and 3) documentation of the completion of required training. In addition, NETPDTC is taking action to conduct a review of all contract employees to verify that all have a background investigation or security clearance on file. NETPDTC will take action to suspend the account of any contract employee who does not have a record of either a background investigation or security clearance in JPAS.

Expected completion of the action is 30 September 2011 for current employees, and will be subject to continuing action thereafter.

NAVAUDSVC Recommendation 3:

Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.

NETPDTC Response:

Concur.

NETPDTC agrees adequate controls should be in place to ensure contractor SAAR-N forms are complete. The NETPDTC Contractor Officer Representative (COR) will:

(1) Develop and implement a process to perform periodic inspections of contractor SAAR-N Forms. The NETPDTC COR has revised the Technical Assistant (TA) appointment letter making the TA responsible for "coordinating" the background/security and SAAR-N information/requirements.

(2) Additionally, the FY12 Task Order will incorporate a paragraph to address these requirements.

Expected completion of the action is 30 June 2012.

NAVAUDSVC Recommendation 4:

Update the local instructions to include, but not limited to: (1) requiring proper completion of System Authorization Access Request-Navy forms before granting system access; (2) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (3) specifying retention period for training documentation as required in the DON Records Management Program.

NETPDTC Response:

Concur.

Although individual (remote) sites will be held responsible to ensure internal controls for system access requirements are in place, NETPDTC agrees final responsibility for the contract employees belongs to the command. NETPDTC COR will:

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

(1) Develop and/or revise local instructions/documents to ensure proper completion of SAAR-N Forms, perform quarterly inspections of contractor SAAR-N Forms, and retention of training documentation.

(2) Additionally, the FY12 Task Order will incorporate a paragraph to address these requirements.

Expected completion of the action is 30 June 2012.

NAVAUDSVC Recommendation 5 and 6 are addressed to the Commander Space and naval Warfare Systems – Atlantic for Action.

NAVAUDSVC Recommendation 5:

Review System Authorization Access Request-Navy documentation for all contract employees for completeness.

SPAWAR Response:

Concur.

SPAWARSYSCEN-Atlantic is currently reviewing all contract employee SAAR-Ns for completeness.

Estimated completion date is 30 June 2012.

NAVAUDSVC Recommendation 6:

Update standard operating procedures to include a requirement for quarterly inspections of System Authorization Access Request-Navy documentation for all new contract employees.

SPAWAR Response:

Concur.

SPAWARSYSCEN-Atlantic is updating its Standard Operating Procedures/Process to include and implement a quarterly review process comparing new contractors with IT access to SAAR-Ns on file.

The update and instantiation of processes will be completed by 30 June 2012.

NAVAUDSVC Recommendation 7 and 8 are addressed to the Commander Office of Naval Intelligence (ONI) for Action.

NAVAUDSVC Recommendation 7:

Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

ONI Response:

Concur.

The Hopper Information Services Center (ISC) is working in concert with the ONI Special Security Office (SSO) to execute a 100 percent inventory of SAAR-N Forms and associated training documentation for all 451 of the contractors who currently have access to the ONI Sensitive but Unclassified Internet Protocol Router Network (NIPRNET).

Estimated completion date for the inventory is 30 September 2011.

NAVAUDSVC Recommendation 8:

Establish written standard operating procedures to include, but not limited to: (1) identifying processes for granting network access; (2) requiring proper completion of System Authorization Access Request-Navy forms; (3) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (4) specifying the retention period for training documentation as required in the DON Records Management Program.

ONI Response:

Concur.

The Hopper ISC is working with ONI claimancy to draft an Office of Naval Intelligence Instruction (ONIINST) that formally codifies a SAAR-N and broader user access management Standard Operating Procedure (SOP) assembled in May 2011 by a command-wide tiger team. The ONIINST is on-track for Commander, Office of Naval Intelligence (COMONI) approval and subsequent promulgation by 31 August 2011.

Estimated completion of actions is 30 September 2011.

~~FOR OFFICIAL USE ONLY~~

Appendix 2:

Management Response from Commanding Officer, Naval Education and Training Professional Development and Technology Center



DEPARTMENT OF THE NAVY
NAVAL EDUCATION AND TRAINING PROFESSIONAL
DEVELOPMENT AND TECHNOLOGY CENTER
1492 SAUFLEY FIELD ROAD
PENSACOLA, FLORIDA 32508-2927

INTER-OFFICE REPORT
7510
N00C
1 JUL 2011

From: Commanding Officer, Naval Education and Training
Professional Development and Technology Center (NETPDTC)
To: Assistant Auditor General for Financial Management and
Comptroller Audits, Naval Audit Service

Subj: NAVAL AUDIT SERVICE DRAFT REPORT ENTITLED "CONTRACTORS
ACCESSING DEPARTMENT OF THE NAVY INFORMATION ON NON-NAVY
MARINE CORPS INTRANET NETWORKS (N2010-NFA000-0066)"

Ref: (a) NAVAUDSVC email of 7 Jun 11
(b) NAVAUDSVC Draft Report of 7 Jun 11

Encl: (1) NETPDTC response to findings
(2) NETPDTC response to recommendations

1. Pursuant to references (a) and (b), NETPDTC responses to the findings and recommendations 2 through 4 are provided in enclosures (1) and (2). Although NETPDTC concurs with the overall findings, explanations are provided regarding the findings via enclosure (1). NETPDTC concurs with recommendations 2 through 4, and has undertaken the appropriate remedies, as discussed in enclosure (2).

2. The NETPDTC point of contact for the responses to the findings and recommendations is [REDACTED] (NETPDTC N641); contact [REDACTED] For audit liaison matters, contact [REDACTED] (NETPDTC N00C), [REDACTED]

[REDACTED]

[REDACTED]

Copy to:
NETC (N00GR)

FOIA (b)6

NETPDTC RESPONSE TO FINDINGS IN NAVAL AUDIT SERVICE DRAFT REPORT
ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

Joint Personnel Adjudication System:

FINDING (page 6): We found that 11 (17 percent) of 66 contract employees had access to the network, but had no record of a favorable adjudication/background investigation.

NETPDTC RESPONSE TO FINDING: Of the 11 contract employees in the sample, 3 of these contractors possessed clearances which were finalized in 2003, 2004, and 2008. Computer Sciences Corporation inadvertently provided incorrect Social Security Numbers to the NAVAUDSVC for 2 of the 3 contractors, which explains the absence of their investigation in Joint Personnel Adjudication System (JPAS). The other contractor had a clearance and NETPDTC does not understand why the NAVAUDSVC was unable to find the clearance in JPAS. The remaining 7 contractors completed their required documentation for a background investigation and submitted their application packages to the security personnel at their (remote) sites. However, the remote site security personnel refused to accept and process the packages. NETPDTC subsequently asked these contractors to send the packages to NETPDTC security personnel for processing. NETPDTC took this step in order to ensure the contractors were appropriately cleared. Currently all of these background investigations have been completed (with no issues) with the exception of 1 investigation still in process. None of the 11 contractors were located at NETPDTC. Although NETPDTC is the Contracting Officer's Representative (COR), the command relies on government oversight of contractors by the local (geographically disbursed) commands that are supported by the contract. Contractors working at remote sites are under the jurisdiction of the command to which they are assigned to support. Local oversight of contract personnel is the responsibility of the command to which the contractors provide support. Commands have been mandated to use the Contractor Verification System (CVS) to facilitate the application, validation, and approval of personnel data for the purpose of issuing a Common Access Card (CAC) to contractor personnel.

Enclosure (1)

~~FOR OFFICIAL USE ONLY~~

The management response from DON CIO is not being treated as FOUO, therefore we are striking the FOR OFFICIAL USE ONLY markings on the management response.

NETPDTC RESPONSE TO FINDINGS IN NAVAL AUDIT SERVICE DRAFT REPORT
ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

Systems Authorization Access Request Form:

FINDING (page 6): In addition, we found that 6 (9 percent) of 66 access request forms were properly processed as required by Commander Naval Network Warfare Command, Computer Tasking Order. However, 57 (86 percent) forms were not. For example, the access request forms: 1) were missing security validations and designation of information technology access level; 2) had no signature of approval by the information assurance manager and/or security manager; or 3) had late signatures of approval.

NETPDTC RESPONSE TO FINDING: Only 5 of the contractor employees who filled out the SAAR forms were located at Pensacola. Of the 5, 2 were located at NAS Pensacola and 1 was located at Corry Station Pensacola. Both of these locations conduct their own security clearance programs. The remaining 2 were located at Saufley Field but 1 was submitted by a Center for Personal and Professional Development (CPPD) employee. The CPPD command has jurisdiction over their SAAR forms. NETPDTC conducted a review of the SAAR document on file for the 1 remaining NETPDTC contractor and found no issues of note. Not all blocks were filled, but the pertinent ones contained appropriate data and the missing blocks were not of legal value or issue. Local and global governance policy/requirements and processes have been strengthened since early implementation and now all blocks are filled for each submitted SAAR form.

Training:

FINDING (Page 7): We found that 36 (55 percent) of 66 contract employees completed required training. However, 25 (38 percent) of 66 contract employees were accessing the network without evidence of required initial training. Specifically, 6 (24 percent) of 25 contract employees were missing required initial personal identifiable information training, and 19 (76 percent) of 25 contract employees were missing both initial information assurance and personal identifiable information training before accessing the network.

NETPDTC RESPONSE TO FINDINGS IN NAVAL AUDIT SERVICE DRAFT REPORT
ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

NETPDTC RESPONSE TO FINDING: Per NETPDTC review of the
NAVAUDSVC sampling list, there was only 1 contractor located at
NETPDTC who had not completed initial PII training. All of the
other 24 contractors were located at other (remote) sites. Our
verification showed all the contractors located at other
Pensacola sites had also completed Information Assurance and
initial PII training.

NETPDTC RESPONSE TO RECOMMENDATIONS IN NAVAL AUDIT SERVICE DRAFT
REPORT ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

1. RECOMMENDATION 2. Suspend network accounts for contract employees who have no record of security clearances/background investigations in the Joint Personnel Adjudication System until issues are resolved.

a. NETPDTC RESPONSE TO RECOMMENDATION 2. CONCUR. NETPDTC agrees that employees without record of security clearance or background investigation in the Joint Personnel Adjudication System should not have network accounts or access to the network. The following corrective action has been taken:

(1) Upon receiving the preliminary audit results last fall, NETPDTC researched the 11 records reviewed in the audit and resolved 10 of the 11 instances of the issue of lack of record of a favorable adjudication/background investigation in November 2010. The record for 1 contract employee listed on the audit sampling has not yet been resolved for a favorable adjudication/background investigation. NETPDTC will suspend the network account for this contract employee by 31 August 2011 if the background investigation has not been resolved at that time. The suspension will continue until all issues have been resolved.

(2) The FY12 Statement of Work for the Computer Science Corporation (CSC) contract requires that all contract employees have a Common Access Card (CAC) before they are allowed on the network (if access is required to perform their job duties).

(3) After the initial audit findings, CSC reviewed all contract employee records for all 400+ contractors hired on the contract and made proper resolutions where necessary regarding 1) documentation of background investigations or security clearances; 2) proper completion of system access forms; and 3) documentation of the completion of required training. In addition, NETPDTC is taking action to conduct a review of all contract employees to verify that all have a background investigation or security clearance on file. NETPDTC will take action to suspend the account of any contract employee who does

Enclosure (2)

~~FOR OFFICIAL USE ONLY~~

NETPDTC RESPONSE TO RECOMMENDATIONS IN NAVAL AUDIT SERVICE DRAFT
REPORT ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

record of either a background investigation or security clearance in JPAS.

b. **TARGET DATE FOR COMPLETION:** Although remedial actions have already taken place, this will be an ongoing effort to ensure continued compliance.

2. **RECOMMENDATION 3.** Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.

a. **NETPDTC RESPONSE TO RECOMMENDATION 3. CONCUR.** NETPDTC agrees adequate controls should be in place to ensure contractor System Authorization Access Request-Navy (SAAR-N) forms are complete. NETPDTC COR will:

(1) Develop and implement a process to perform periodic inspections of contractor SAAR-N Forms. The NETPDTC COR has revised the Technical Assistant (TA) appointment letter making the TA responsible for "coordinating" the background/security and SAAR-N information/requirements.

(2) Additionally, the FY12 Task Order will incorporate a paragraph to address these requirements.

b. **TARGET DATE FOR COMPLETION:** 31 December 2011

3. **RECOMMENDATION 4.** Update local instructions to include, but not limited to: 1) requiring proper completion of System Authorization Access Request-Navy forms before granting system access; 2) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and 3) specifying retention period for training documentation as required in the DON Records Management Program.

a. **NETPDTC RESPONSE TO RECOMMENDATION 4. CONCUR.** Although individual (remote) sites will be held responsible to ensure internal controls for system access requirements are in place, NETPDTC agrees final responsibility for the contract employees belongs to the command. NETPDTC COR will:

2

Enclosure (2)

~~FOR OFFICIAL USE ONLY~~

NETPDTC RESPONSE TO RECOMMENDATIONS IN NAVAL AUDIT SERVICE DRAFT
REPORT ENTITLED "CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY
INFORMATION ON NON-NAVY MARINE CORPS INTRANET NETWORKS
(N2010-NFA000-0068)

(1) Develop and/or revise local instructions/documents to ensure proper completion of SAAR-N Forms, perform quarterly inspections of contractor SAAR-N Forms, and retention of training documentation.

(2) Additionally, the FY12 Task Order will incorporate a paragraph to address these requirements.

b. TARGET DATE FOR COMPLETION: 31 December 2011

3

Enclosure (2)

~~FOR OFFICIAL USE ONLY~~

Appendix 3:

Management Response from Commander, Space and Naval Warfare Systems Command



DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

7500
Ser 8.6/023
11 Jul 2011

FIRST ENDORSEMENT on SPAWAR Systems Center Atlantic ltr
7500 Ser 86/02461 of 6 Jul 11

From: Commander, Space and Naval Warfare Systems Command
To: Assistant Auditor General for Financial Management and
Comptroller Audits, Naval Audit Service

Subj: NAVAL AUDIT SERVICE (NAVAUDSVC) DRAFT AUDIT REPORT ON
CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION
ON NON-NAVY MARINE CORPS INTRANET NETWORKS, PROJECT NO.
N2010-NFA000-0068, DATED 7 JUNE 2011

1. Forwarded with concurrence.
2. Questions concerning this correspondence may be directed to
[REDACTED] SPAWAR Inspector General, at [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
Deputy Commander

Copy to:
SPAWAR Systems Center Atlantic
OPNAV N2/N6

FOIA (b)6

The management response from SPAWAR is not being treated as FOUO, therefore we are striking the FOR OFFICIAL USE ONLY markings on the management response. However, we are marking this page of the report FOUO because the management response contains personally identifiable information that is exemption from release under Freedom of Information Act Exemption (b)6.

~~FOR OFFICIAL USE ONLY~~

FOR OFFICIAL USE ONLY



DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

7500
Ser 8.6/023
11 Jul 2011

FIRST ENDORSEMENT on SPAWAR Systems Center Atlantic ltr
7500 Ser 86/02461 of 6 Jul 11

From: Commander, Space and Naval Warfare Systems Command
To: Assistant Auditor General for Financial Management and
Comptroller Audits, Naval Audit Service

Subj: NAVAL AUDIT SERVICE (NAVAUDSVC) DRAFT AUDIT REPORT ON
CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION
ON NON-NAVY MARINE CORPS INTRANET NETWORKS, PROJECT NO.
N2010-NFA000-0068, DATED 7 JUNE 2011

1. Forwarded with concurrence.
2. Questions concerning this correspondence may be directed to
[REDACTED] SPAWAR Inspector General, at [REDACTED]
[REDACTED]

FOIA (b)6

[REDACTED]
[REDACTED]
Deputy Commander

Copy to:
SPAWAR Systems Center Atlantic
OPNAV N2/N6

~~FOR OFFICIAL USE ONLY~~

**Space and Naval Warfare Systems Center Atlantic Response to
Recommendation in Naval Audit Service Draft Audit Report
N2010-NFA000-0068**

**We recommend that Executive Director, Space and Naval Warfare
Systems Center - Atlantic:**

Recommendation 5. Review System Authorization Access Request-
Navy documentation for all contract employees for completeness.

Response: Concur. SPAWARSYSCEN Atlantic is currently reviewing
all contract employee SAAR-Ns for completeness. Estimated
completion date is 31 May 2012.

Recommendation 6. Update standard operating procedures to
include a requirement for quarterly inspections of System
Authorization Access Request-Navy documentation for all new
contract employees.

Response: Concur. SPAWARSYSCEN Atlantic is updating its
Standard Operating Procedures/Process to include and implement a
quarterly review process comparing new contractors with IT
access to SAAR-Ns on file. Update and instantiation of process
will be completed by 31 May 2012.

Enclosure (1)

Appendix 4:

Management Response from Commander, Office of Naval Intelligence



DEPARTMENT OF THE NAVY
OFFICE OF NAVAL INTELLIGENCE
4251 SULLY ROAD
WASHINGTON, D.C. 20395-5720

IN REPLY REFER TO
7510
Ser 00/ 110
28 Jun 11

From: Commander, Office of Naval Intelligence
To: Assistant Auditor General for Financial Management and
Comptroller Audits

Subj: CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION
ON NON-NAVY MARINE CORPS INTRANET NETWORKS (DRAFT AUDIT
REPORT N2010-NFA000-0068)

Ref: (a) NAVAUDSVC memo 7510 N2010-NFA000-0068 of 7 Jun 11

Encl: (1) Office of Naval Intelligence (ONI) Response to
Findings and Recommendations

1. As requested by reference (a), enclosure (1) provides our
response to the findings and recommendations contained in
subject report.

2. The ONI point of contact for this issue is [REDACTED]
ONI-232, [REDACTED] UNCLASS Internet
address [REDACTED]

[REDACTED]
[REDACTED]
Deputy

Copy to:
NAVINGEN (04)
[REDACTED] ISC
ONI CIO
ONI MSD

FOIA (b)6

FOIA (b)6

The management response from ONI is not being treated as FOUO, therefore we are striking the FOR OFFICIAL USE ONLY markings on the management response. However, we are marking this page of the report FOUO because the management response contains personally identifiable information that is exemption from release under Freedom of Information Act Exemption (b)6.

~~FOR OFFICIAL USE ONLY~~

OFFICE OF NAVAL INTELLIGENCE (ONI) RESPONSE

DRAFT AUDIT REPORT N2010-NFA000-0068
CONTRACTORS ACCESSING DEPARTMENT OF THE NAVY INFORMATION ON
NON-NAVY MARINE CORPS INTRANET NETWORKS

ONI-SPECIFIC FINDINGS/CONCLUSIONS AND RECOMMENDATIONS

Finding - Authorization for Access

Auditors reviewed 66 of 183 contract employees who had access to one of the ONI networks. Auditors determined that ONI had no local guidance on the complete process of granting network access. The command follows an unwritten procedure for granting contract employees access to any of their networks.

Joint Personnel Adjudication System (JPAS). ONI requires specific security access and a Single Scope Background Investigation prior to gaining access to their network. All 66 contract employees had the specific security adjudication and background investigation records in JPAS.

Systems Authorization Access Request-Navy (SAAR-N) Form. ONI was able to provide 39 of the 66 SAAR-N forms requested. The command had no documentation for the remaining 27 contract employees. Of the 39 SAAR-N forms received, none of them were properly completed and processed. This occurred because personnel were unaware of the access request form requirement; not reviewing forms; and not documenting approvals.

Information Assurance (IA) Training. Auditors verified that 47 of 66 contract employees had evidence of initial IA training required by DoD Instruction 8570.01-M. However, 19 contract employees were accessing the network without any evidence of required initial IA training. This occurred because contract employees were not taking the training or command personnel were not maintaining required documentation.

ONI Comments: Concur.

Conclusion. Opportunities exist to improve DON's process of granting contractor and subcontractor personnel access to information on non-Navy Marine Corps Intranet networks. The need to properly authorize and receive appropriate training to access networks is a concern throughout DON. Auditors found that (1) contract employees did not have documented background

~~FOR OFFICIAL USE ONLY~~

ENCLOSURE()

investigations or security clearances prior to accessing the network; (2) system access forms were incomplete, inaccurate, or missing; and (3) contract employees had not completed the required initial training.

ONI Comments: Concur with Conclusions (2) and (3). Conclusion (1) does not apply, as ONI requires specific security access and a Single Scope Background Investigation prior to gaining access to our network.

ONI-specific Recommendations

Note - Recommendations 1 through 6 of this report do not apply to ONI or its echelon III organizations.

7. Review System Authorization Access Request-Navy and training documentation for all contract employees for completeness.

ONI Comments: Concur. Hopper ISC is working in concert with the ONI Special Security Office (SSO) to execute a 100 percent inventory of System Authorization Access Request-Navy (SAAR-N) forms and associated training documentation for all 451 of the contractors who currently have access to the ONI Sensitive but Unclassified Internet Protocol Router Network (NIPRNET). Estimated completion date for the inventory is 8 Jul 2011.

8. Establish written standard operating procedures to include, but not limited to: (1) identifying processes for granting network access; (2) requiring proper completion of System Authorization Access Request-Navy forms; (3) requiring quarterly inspection of System Authorization Access Request-Navy and training documentation for all new contract employees; and (4) specifying the retention period for training documentation as required in the DON Records Management Program.

ONI Comments: Concur. Hopper ISC is working with the ONI claimancy to draft an Office of Naval Intelligence Instruction (ONIINST) that formally codifies a SAAR-N and broader user access management Standard Operating Procedure (SOP) assembled in May 2011 by a command-wide tiger team. The ONIINST is on-track for Commander, Office of Naval Intelligence (COMONI) approval and subsequent promulgation by 31 Aug 2011.

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies

of this document

~~FOR OFFICIAL USE ONLY~~