

Naval Audit Service



Audit Report



Navy/Marine Corps Intranet Internal Controls Over Computers During Turn-In Process

This report contains information exempt from release under the Freedom of Information Act. Exemption

~~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~~

N2011-0025
18 March 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
N2009-NFO000-0063.001
18 Mar 11

MEMORANDUM FOR DEPARTMENT OF THE NAVY PROGRAM EXECUTIVE
OFFICE FOR ENTERPRISE INFORMATION SYSTEMS
COMMANDER, NAVY CYBER FORCES
COMMANDANT OF THE MARINE CORPS

Subj: **NAVY/MARINE CORPS INTRANET INTERNAL CONTROLS OVER
COMPUTERS DURING TURN-IN PROCESS (AUDIT REPORT
N2011-0025)**

Ref: (a) NAVAUDSVC memo N2009-NFO000-0063, dated 15 Jan 2009
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

1. The report provides results of the subject audit announced in reference (a). Section A of this report provides our finding and recommendations. Recommendations 1 through 7 were addressed to the Department of the Navy Program Executive Office for Enterprise Information Systems. Recommendations 8 through 10 were addressed to the Office of the Commander, Navy Cyber Forces. Recommendations 11 and 12 were addressed to the Commandant of the Marine Corps.

2. We did not receive formal signed management responses from any of the commands. Therefore, all 12 recommendations are considered undecided and are being resubmitted to the applicable commands for response. The commands are required to provide responses to the undecided recommendations within 30 days.

3. Please provide all correspondence to the Assistant Auditor General for Manpower and Reserve Affairs Audits, XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX, with a copy to the Director, Policy and Oversight, XXXXXXXXXXXXXXXXXXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)

FOIA (b)(6)

4. Any requests for this report under the Freedom of Information Act must be approved by the Auditor General of the Navy as required by reference (b). This audit report is also subject to followup in accordance with reference (b).

Subj: **NAVY/MARINE CORPS INTRANET INTERNAL CONTROLS OVER
COMPUTERS DURING TURN-IN PROCESS (AUDIT REPORT
N2011-0025)**

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



FOIA (b)(6)

XXXXXXXXXXXXXXXXXXXXX
Assistant Auditor General
Manpower and Reserve Affairs Audits

Copy to:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N4B, N40, N41)
CMC (ACMC)
COMFLTFORCOM
DON CIO
NAVINGEN (NAVIG-4)
AFAA/DO

Table of Contents

SECTION A: FINDING, RECOMMENDATIONS, AND CORRECTIVE ACTIONS	1
Finding: Navy/Marine Corps Intranet Tech Refresh Computers Not Fully Accounted For	1
Reason for Audit.....	1
Synopsis.....	1
Background.....	3
Audit Results	3
Recommendations and Corrective Actions	13
SECTION B: STATUS OF RECOMMENDATIONS.....	17
EXHIBIT A: BACKGROUND.....	21
EXHIBIT B: PERTINENT GUIDANCE.....	23
EXHIBIT C: SCOPE AND METHODOLOGY.....	25
Scope	25
Methodology.....	25
Federal Managers’ Financial Integrity Act.....	27
EXHIBIT D: ACTIVITIES VISITED AND/OR CONTACTED	28
EXHIBIT E: SURVEY COMMENTS.....	30

Section A:

Finding, Recommendations, and Corrective Actions

Finding: Navy/Marine Corps Intranet Tech Refresh Computers Not Fully Accounted For

Reason for Audit

The audit objective was to verify that the internal controls over Navy/Marine Corps Intranet (NMCI) computers during the tech refresh turn-in process¹ are sufficient to safeguard Department of Navy (DON) information and personally identifiable information (PII).

Both the Government Accountability Office and DON identified safeguarding PII as a high-risk area.² We regard the NMCI tech refresh turn-in process as high-risk due to the potential loss or theft of computers containing personally identifiable information, as well as DON information, on the hard drives. This audit is a follow-on to a prior Naval Audit Service audit, “Processing of Computers and Hard Drives During the Navy/Marine Corps Intranet Computer Disposal Process,” (N2009-0027, 28 April 2009).³ It is one of a series of Naval Audit Service-initiated audits being undertaken to verify that sensitive DON information and personally identifiable information are properly safeguarded.

Synopsis

DON was unable to know whether computers turned in during the tech refresh process were fully accounted for and that DON official information and personally identifiable information were properly safeguarded. These conditions occurred because DON and the NMCI contractor had not established and executed uniform and specific tech refresh turn-in policies and procedures. Specifically, neither DON nor its contractor established detailed procedures to verify that hard drives assigned to turned-in computers were, in

¹Technology (Tech) Refresh is the periodic upgrade of existing NMCI workstations with new hardware to provide increased technological capabilities and performance for NMCI users. After the upgrade, the next step is turn-in, in which the old computers are collected and shipped to their disposition point. Each old computer is tracked by an Asset Tag number throughout the process.

²Office of Management and Budget Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” defines PII as “information which can be used to distinguish or trace an individual’s identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”

³The recommendations in report N2009-0027 addressed controls over the disposition of hard drives during the disposal process, which takes place after the Tech Refresh turn-in process.

fact, inside the computers. Pickup and followup procedures for computers were not sufficiently detailed and standardized to account for all turned-in computers. Specific roles and responsibilities for handling computers that are not picked up were not well defined in policy. Physical inventories and Seat Deployment Schedule⁴ listings were not reconciled, and contractor and DON databases that track computers contained inaccurate information. We found that for the period of 31 March 2008 through 1 May 2009, of 99,791⁵ computers available for the tech refresh turn-in process, 19,880 (20 percent) could not be accounted for using official contractor records. We also learned of multiple instances of computers being stolen from various locations during the tech refresh process. The incidents involved the theft of an estimated 297 computers or standalone hard drives, only 45 of which were recovered. It is not known whether the unrecovered computers/hard drives were encrypted or reformatted, nor what, if any, data or PII was stored on them. Because neither DON nor its NMCI contractor, Hewlett-Packard Enterprise Services,⁶ had asset management and accountability systems that could reconcile turned-in computers, neither one of them was able to detect the missing computers.

DON information assurance policies⁷ require the proper safeguarding of DON data and PII. Because DON was unable to know when computers were missing, lost, or stolen, DON PII and other sensitive data was exposed to an unacceptable risk. The loss or compromise of only one computer hard drive⁸ with unencrypted data can result in a data breach, identity theft, public embarrassment, and harm to DON and its military and civilian employees. Given the nature of the conditions found during the audit and the subsequent thefts and reported history of thefts, we concluded that shortcomings in DON's NMCI asset accountability and management represents a significant DON-wide internal control weakness.

Command Ethics Program. During the audit, we also reviewed the Norfolk Naval Station's ethics program. We determined that the command did have an effective ethics program in place in terms of the systems, processes, procedures, etc., to reasonably ensure compliance with DoD 5500.7-R, "Joint Ethics Regulation," and Executive Order 12674, "Principles of Ethical Conduct for Government Officers and Employees" as modified by Executive Order 12731.

⁴The Seat Deployment Schedule is the schedule that will provide the exact seat (contractor-owned desktops and laptops, and other computing hardware, software, and related services bundled and provided at a fixed price per unit), date, and location of refresh. It also provides information on the retiring asset such as Asset Tag number and Machine Name.

⁵Figures are from the Executive Program Office Actuals reports for the period 31 March 2008 - 1 May 2009 that Hewlett-Packard Enterprise Services reported as deployed computers.

⁶Hewlett-Packard Enterprise Services was formerly the EDS business unit of Hewlett-Packard.

⁷Secretary of the Navy Instruction 5211.5E, "Department of the Navy (DON) Privacy Program," 28 December 2005; Secretary of the Navy Instruction 5239.3A, "Department of the Navy Information Assurance (IA) Policy," 20 December 2004, etc. See also Exhibit B.

⁸See Naval Audit Service report N2009-0027, "Processing of Computers and Hard Drives During the Navy/Marine Corps Intranet (NMCI) Computer Disposal Process," 28 April 2009, which found improperly sanitized unclassified hard drives containing personally identifiable information, as well as 14 unsecured classified hard drives containing "Secret" documents.

Background

Navy Cyber Forces and the Commandant of the Marine Corps are each responsible for information security programs and operational instructions in their respective services.

The Space and Warfare Systems Command Program Executive Office for Enterprise Information Systems had overall responsibility for the NMCI computers. The Space and Naval Warfare Systems NMCI Program Manager (PMW-200) had overall management responsibility for NMCI and the prime contractor who operated NMCI. We kept both offices informed of our progress throughout the audit. The program office was instrumental in helping the team collect the data used for analysis. Exhibit A provides a more detailed explanation of the tech refresh process.

Audit Results

DON was unable to know whether computers turned in during the tech refresh turn-in process were fully accounted for and that DON official information and personally identifiable information were properly safeguarded. Although DON did not own the computers, DON information assurance policies and its NMCI contract with Hewlett-Packard Enterprise Services require the proper safeguarding of official DON information and PII with sound accountability procedures. However, shortcomings in DON's NMCI asset accountability and management procedures allowed this condition to exist. As a result, during the tech refresh turn-in process, DON was not made aware of computer thefts and of the significant risk of stolen and/or compromise of personally identifiable information and other sensitive data. A recent incident at the Enterprise Warehouse in Mechanicsburg, PA involved the theft of an estimated 150 computers. Although 15 of the stolen computers were recovered and found to contain encrypted data, DON was unable to know whether or not data on the other 135 unaccounted-for computers were encrypted. Another estimated 147 computers were stolen from Naval Support Activity Millington, TN during a 2-month period, with an unknown number of additional thefts apparently occurring for nearly 3 years. Twenty-seven computers and three standalone hard drives were recovered, but the number of unencrypted stolen computers and hard drives is unknown. Hewlett-Packard Enterprise Services was unaware of any of these thefts due to their asset management and accountability system not being able to detect unaccounted-for computers. These incidents highlight the unacceptable vulnerabilities in the current internal control process, susceptibility to theft of computers, and lack of procedures and systems to detect or identify missing computers.

Hard Drives Not Checked During Turn-In Process

We found that as computers were picked up from each activity and transported during the tech refresh turn-in process, the computers were not checked to determine whether they contained a hard drive⁹ until arriving at the Enterprise Warehouse, which was months later.¹⁰ Further, the contractor did not follow up on or inform DON about missing hard drives. If a computer was found without a hard drive, contracting personnel installed another hard drive into the computer and the computer continued through the sanitization process as a complete unit. There was no specific DON or Hewlett-Packard Enterprise Services policy, procedure, or contract provision established to check for or report missing hard drives for turned-in computers. The contractor stated that “there is no policy that requires Electronic Data Systems¹¹ to check the returned seat¹² to validate the hard drive is in the seat. If a hard drive is missing from the computer casing, it is discovered during the Sanitization process.” DON information security guidance requires the protection of DON and privacy information.¹³ The NMCI contract provisions require the contractor to develop procedures and implementation plans to ensure that information technology resources leaving the control of the assigned user are cleared of all DON data. In practice, computers/hard drives were not sanitized until they reached the Enterprise Warehouse in Mechanicsburg, which, as noted, could be months after they were picked up at the using activity.

Hewlett-Packard Enterprise Services did not know how many computers were, or would be, turned in and picked up without their assigned hard drive. Therefore, they would not know how many hard drives were missing, lost, or stolen because no controls existed to identify, track, or report those hard drives. This represents a significant systemic risk to DON that can result in undetected stolen hard drives, data compromise, loss of personally identifiable information, identity theft, and increased reputational risks.

As a result of our earlier audit on the disposal of hard drives, and subsequent to our field work for this audit, DON began a change to the tech refresh process under which refreshed hard drives are not collected by the contractor, but are instead retained by the applicable DON command. Computers will continue to be collected by the contractor and taken to cross-dock warehouses and the Enterprise Warehouse. Because the change in the tech refresh process to address the issue of missing hard drives was begun as a result of the previous audit, we are not making a recommendation in this report regarding

⁹Recommendation #3 from N2009-0027 “Processing of Computers and Hard Drives During the Navy Marine Corps Intranet (NMCI) Computer Disposal Process,” states, “Develop policy that requires the tracking (by serial or other identifying number) of all hard drives (classified and unclassified) once separated from a computer. “ DON has issued this policy, DON CIO WASHINGTON DC 221633Z AUG 10 PROCESSING OF MAGNETIC HARD DRIVE STORAGE MEDIA FOR DISPOSAL.

¹⁰The contractor estimates the average time for a computer to reach Mechanicsburg after Tech Refresh to be 2 months. This does not include computers not picked up at the scheduled time, which take longer to reach Mechanicsburg, and computers not picked up at all.

¹¹Hewlett-Packard Enterprise Services was formerly the Electronic Data Systems business unit of Hewlett-Packard.

¹²A “seat” is a contractor-owned desktop or laptop, or other computing hardware, software, and related services bundled and provided on a fixed price per unit.

¹³Secretary of the Navy Instruction 5211.5E, “Department of the Navy (DON) Privacy Program,” 28 December 2005; Secretary of the Navy Instruction 5239.3A, “Department of the Navy Information Assurance (IA) Policy,” 20 December 2004, etc.

the reporting of unclassified missing hard drives to the originating activity for followup. Our remaining recommendations reflect this revised process, which is still being implemented.

During our audit, DON implemented the Data at Rest solution, which represents the DON Risk Mitigation Strategy to safeguard data on each NMCI network computer.¹⁴ It is unknown how many, if any, computers that were refreshed during the last 3 months of our audit scope period were likely to have been encrypted by Data at Rest.¹⁵ We were informed by NMCI personnel that Data at Rest had been implemented on about 90 percent of NMCI computers as of 1 May 2010. The Data at Rest initiative should provide protection of data on encrypted hard drives that are turned in during tech refresh. However, hard drives on which Data at Rest has not yet been implemented, as well as computers that had been removed from the network for tech refresh prior to Data at Rest implementation but had not been picked up by Hewlett-Packard Enterprise Services, lack encryption, and could still be at risk. Further, it cannot be guaranteed how long the Data at Rest encryption technology will remain viable. Therefore, there remains a need for strengthened controls over the possession and tracking of hard drives and computers during the tech refresh process.

Lack of Pickup and Followup Policies and Procedures

We found no written, detailed, standardized tech refresh turn-in and pickup policy and procedures instructing contractor or DON personnel on procedures to follow during the tech refresh turn-in process. Contract technical representatives¹⁶ and activity personnel with tech refresh duties at each location we visited told us that they were unaware of any standardized pickup and followup procedures. Ninety-six percent of those who responded to our survey questionnaire¹⁷ stated that no documentation was received at the time of computer pickup, and 54 percent reported that the contractor had not picked up the computers within the required 24-hour¹⁸ period. Thirty respondents offered suggestions for improvement, and 72 percent agreed that a need exists for specific pickup and followup procedures and documentation. Questionnaire responses included the following observations:

- “Records and accountability for assets is terrible.”

¹⁴Data at Rest is being implemented on the NMCI network first followed by the Navy One-Net, IT-21, and Marine Corps MCEN networks. One-Net, IT-21, and Marine Corps MCEN networks were not part of this audit.

¹⁵There was a 3-month overlap period for Data at Rest implementation and our audit scope period. Data at Rest implementation began February 2009 for the USMC and March 2009 for the USN, and our scope period for testing ended 1 May 2009.

¹⁶An NMCI contract technical representative is generally the user point of contact for any changes to the NMCI computer hardware, software, and related services.

¹⁷See Exhibit C: Scope and Methodology for explanation of the survey. We received 119 responses of 189 survey sent (63 percent return rate).

¹⁸The NMCI Contract Technology Refresh Lifecycle and Discipline Guide, 8 February 2008 requires “Retiring assets will be picked up by EDS within 24 hours of refresh, unless otherwise requested at RM3 and coordinated between the EDS RPM and the contract technical representative. As a rule, the asset should not be left for greater than 3 business days.”

- “Standardize tech refresh pick up process and documentation for all sites.”
- “I noticed a couple of times, the tech refresh deployer took a retired asset without looking at the asset number on the computer.”
- “Once the replacement was received, there was no accountability for retrieving the old asset.”
- “Contractor could give receipts to command when picked up.”

See Exhibit E, “Survey Comments,” for additional comments received that support the need for improvements in pickup and followup procedures.

We found that monitoring and control practices varied among installations. Naval Sea Systems Command headquarters, located at the Washington Navy Yard, DC, exercised control by centralizing oversight for all tech refreshed computers before the contractor pickup crew arrived. The process was closely monitored by Naval Sea Systems Command personnel to ensure that computer Asset Tag numbers were verified and all computers were picked up. Naval Station Norfolk, unlike Naval Sea Systems Command headquarters, did not closely monitor and control the pickup process. Pickup crews at Naval Station Norfolk were unescorted to the work areas where refreshed computers had been left for pickup and no personnel ensured that computers were picked up or that the Asset Tag numbers were verified. We found that the pickup crews did not always check computers packed in boxes to verify the accuracy of asset identification information. While there is no specific requirement for the pickup crews to be escorted during the pickup process, in our opinion, it is a reasonable business practice for a command to provide a measure of control and ensure that computers are all picked up and none left behind. Also, command personnel may be able to provide assistance in dealing with some situations that may occur during tech refresh, such as computers left in locked offices, or employees who do not want to relinquish their computers (both of which were reported to us, anecdotally, as situations encountered by Hewlett-Packard Enterprise Services personnel).

Because Hewlett-Packard Enterprise Services was not required to provide commands with custody documentation for each turned-in computer, the commands lost visibility and control of the computers after they were picked up. The commands had no method of monitoring or tracking pickup of the old computers after the tech refresh was performed. Once disconnected from the network, the computers were no longer effectively tracked as assets potentially containing sensitive DON data and personally identifiable information.

Inconsistent procedures and business practices between commands and Hewlett-Packard Enterprise Services cross-dock¹⁹ warehouses resulted in computers not being picked up by Hewlett-Packard Enterprise Services and being left behind at activities. Once a scheduled pickup date passed, some computers remained at the commands for years after the tech refresh. For example, during a visit to Marine Corps Combat Development Command at Quantico, VA we found six old computers that had been refreshed over 2 years before that were scattered about under desks or in locked and unlocked store rooms and offices. We also found a desktop computer in the contract technical representative's office that had been refreshed 18 months earlier. Four U.S. Marine Corps Forces, Pacific activities reported to us that 73 computers were left from various tech refreshes: 39 related to tech refreshes that had occurred in the previous 5-26 months, and 34 for which they reported no specific tech refresh date. These 73 are only those computers that the activity personnel were able to observe at the time of our inquiry. The Marine Corps Forces, Pacific point of contact stated that to gain an accurate count of all left-behind computers they "would have to send a team into every room, of every building, of every base" in Marine Corps Forces, Pacific. Given the number of left-behind computers in our limited audit, extrapolated by the numbers of activities, computers, and tech refreshes for the NMCI network, in our judgment, computers not picked up by Hewlett-Packard Enterprise Services could potentially number hundreds of computers left behind at the activities after tech refresh.²⁰ This poses another significant risk of compromised DON sensitive data and PII, because the computers were not accounted for, and, therefore, did not go through the sanitization and disposal processes.

The contractor guidance, "Technology Refresh Lifecycle and Discipline Guide" and "NMCI Warehouse Operations Playbook," state only that refreshed computers are to be picked up within 24 hours of their refresh and be left at the activity no more than 3 days. The "NMCI Warehouse Operating Procedures" manual shows the documentation and procedures "to correctly and methodically account for assets" once in the warehouses, but they do not completely address tech refresh turn-in items.

Detailed standardized pickup and followup procedures are risk management controls to help prevent mistakes and ensure consistency in operations. A lack of these controls increases the risk of unauthorized disclosures of sensitive DON information and PII, and presents an unnecessary reputational risk to DON.

¹⁹Cross-dock warehouses are temporary facilities used as a transfer point between the military installations and the Enterprise Warehouse in Mechanicsburg, PA. There are nine permanent cross-dock warehouses used by the contractor for the purpose of computer movement. Temporary cross-docks, without Warehouse Management System access, are established for the duration of a Tech Refresh at some installations that are too far from one of the permanent warehouses to be supported.

²⁰The extrapolated conclusion is based on auditor reasoning from observed data.

Lack of Physical Reconciliations

Enterprise Warehouse personnel did not reconcile the physical number of computers they received from the activities with the Seat Deployment Schedule pickup listings or with the number of computers actually scanned into the UniCODE Warehouse Management System.²¹ When computers arrived at a warehouse, they remained there for approximately 2 to 4 days before they were scanned into the Warehouse Management System. This vulnerability was exploited²² at Mechanicsburg by an Enterprise Warehouse worker, who admitted stealing an estimated 150 laptop computers after they had been unloaded from the trucks but before they were scanned into the Warehouse Management System. Because physical reconciliations had not been done, Hewlett-Packard Enterprise Services was unaware of the theft until informed by local law enforcement and base command personnel. Only 15 of the 150 computers were recovered. Although the data on these 15 computers was encrypted, DON was unable to verify that data on the estimated 135 unaccounted for computers was also encrypted. An official in the NMCI Program Manager office who was briefed on the incident estimated that at least 40 of the 135 stolen computers may have been unencrypted. However, the exact number cannot be determined because, due to weaknesses in the turn-in process, Hewlett-Packard Enterprise Services could not identify from their records the specific computers stolen.

At Millington, TN subcontractor personnel exploited a similar weakness in the turn-in process. In this incident (reported to us in September 2010), an estimated 147 computers and stand-alone hard drives that were collected from 10 activities at Naval Support Activity Mid-South were stolen by the Hewlett-Packard Enterprise Services subcontractor employees instead of being inventoried and shipped to Mechanicsburg for sanitization. Three standalone hard drives and 27 computers were recovered. The Naval Criminal Investigative Service discovered personally identifiable information on one standalone hard drive and one computer, including a resume and files containing what they described as “a considerable amount of personally identifiable information.” The Naval Criminal Investigative Service found that the other recovered computers and drives were either encrypted or had been reformatted. It is not known whether the hard drives on the 120 unrecovered computers were encrypted or reformatted. The workers arrested for the theft also reported to the Naval Criminal Investigative Service that they had stolen computers at New Orleans and at every other installation at which they had worked for 3 or 4 years. Hewlett-Packard Enterprise Services was unaware of these thefts due to their asset management and accountability system not being able to detect unaccounted-for computers.

²¹The Warehouse Management System is the database used by the cross-dock and Enterprise warehouses to track computers as they move through the warehouses. Items are scanned in and the data from Warehouse Management System is uploaded into and verified by Asset Center as transactions are processed.

²²The incident was reported to us in June 2010.

The “NMCI Warehouse Operating Procedures” manual does not provide for physical reconciliations for tech refresh turn-in equipment. However, it does state that “It is the responsibility of the lead to ensure that all assets coming into the warehouse are fully accounted for and that all discrepancies in product being received will be brought up to the Warehouse Manager as soon as identified. All products coming into the warehouse should be processed and validated within 24 hours.” This cannot be done effectively unless there is a physical reconciliation between what was shipped to the warehouses, what was actually received, and what was processed through the warehouses.

Lack of internal controls over detection of a missing computer exposes DON to continuing risk of computer thefts, data breaches, identity thefts, and increased reputational risks.

Accuracy of Contractor Data

Contractor records were not complete, not accurate, and did not properly account for all NMCI computers. The contractor was not able to use its records to ensure that all computers were sufficiently safeguarded, and thus was not able to provide the DON full assurance that the computers, personally identifiable information, and DON sensitive information were accounted for and protected. Contractor computer records are critically important and are key to effective asset management. They track and record the status and physical location of each computer during the tech refresh turn-in process, and should be able to be used to alert contractor management and DON of missing, stolen, or lost computers.

We could not reconcile and account for 19,880 (20 percent) of 99,791 computers reportedly available for tech refresh during our scope period of 31 March 2008 to 1 May 2009. We analyzed computer record data listings from four contractor databases²³ and the DON NMCI Enterprise Tool database to test the data reliability and account for these computers. The computer record data field that contained the Asset Tag number, a unique identifier for each computer, was used to perform tests between the DON and contractor information systems for each turned-in computer.

We then presented our results to Hewlett-Packard Enterprise Services for them to explain the apparent discrepancies. Hewlett-Packard Enterprise Services reported being able to reconcile 10,268 with their records, but was unable to account for the remaining 9,612 computers, or about 10 percent of the computers documented in their records. Notable test results included:

- 91 computers processed through the Warehouse Management System, which indicated actual receipt at a cross-dock warehouse, were missing from the Asset

²³UniCODE Warehouse Management System, Seat Deployment Schedule Pick Up Reports, Order Installation Confirmation system, and Asset Center.

Center²⁴ data, which indicated that they were not received at the Enterprise Warehouse. Hewlett-Packard Enterprise Services reported they were able to reconcile all but three of these computers.

- 4,585 computer records listed in the Seat Deployment Schedule pickup reports²⁵ as physically picked up were missing from the Warehouse Management System and Asset Center data, which indicated that they were never received or were never entered into the system at either the cross-dock or Enterprise warehouses. After we provided our results, Hewlett-Packard Enterprise Services reported that they were able to reconcile most, but were not able to account for 152 computers.
- 362 computers were reported as received at the warehouses before they were reported as picked up on the cross-dock Seat Deployment Schedule pickup reports. The time spans ranged from 1 day to 32 months. Hewlett-Packard Enterprise Services' official response to this finding was not specific and conclusive. They stated that "Machines might have been reimaged and redeployed with the same Asset Tag number. These machines with the same Asset Tag numbers may be shown for items coming in and going out."
- 5,902 computers were reported in the Order Installation Confirmation²⁶ data as refreshed, but there was no record of them in the Asset Center. After we provided our results, Hewlett-Packard Enterprise Services reported they were able to reconcile most, but could not account for 155 of the computers.
- 8,940 computer records were mismatched between the Hewlett-Packard Enterprise Services Asset Center records and DON NMCI Enterprise Tool records. The Enterprise Tool data file had 5,674 computers that were missing from the Asset Center, and the Asset Center had 3,266 that were missing from the Enterprise Tool. The Asset Center feeds its data to the Enterprise Tool, so the Asset Tag numbers should match in both systems. Hewlett-Packard Enterprise Services declined to try to reconcile the files, saying that because they had not generated the Enterprise Tool file data they could not stand behind any reconciliation.
- Asset Tag number discrepancies (i.e., invalid or missing Asset Tag numbers) were found in all five information systems (contractor and Enterprise Tool). However, among all of the discrepancies, Warehouse Management System and Asset Center data each displayed a set of discrepancies of exactly the same number (1,320 entries) and type. The 4 most frequently recurring examples of

²⁴Asset Center is the Single Asset Repository for NMCI supporting the lifecycle functions of NMCI assets, inventory, physical location, invoicing, and disposition. This maintains the records and status of the asset throughout the lifecycle.

²⁵Seat Deployment Schedule pickup reports are Excel spreadsheet reports generated weekly by the warehouse managers and reported to the Operations Manager. Hard copy worksheets are given to the pickup crews who manually annotate the worksheet as they pick up computers. The warehouse manager manually enters this information into an Excel computer file daily. The Operations Manager summarizes the reports from all warehouses into an East Coast/West Coast Summary Report. According to the Operations Manager, this report is not used for any further reporting or decision making.

²⁶This system processes the orders for tech refresh computers through actual deployment of the new computer at the user's workstation, and then provides asset data that is used to update the Asset Center.

these discrepancies accounted for 97 percent of the 1,320 discrepancies (shown in Figure 1).

Figure 1. Asset Tag number discrepancies.

ASSET TAG # DISCREPANCIES	ASSET CENTER	Warehouse Management System
0000000000	152	152
3000000000	184	184
"MLSD"	883	883
<Blanks>	71	71
Total	1,290	1,290

An Asset Tag number is the most critical data element because it is the unique identifier to account for and track a computer throughout its life cycle. When asked to explain the errors, Hewlett-Packard Enterprise Services explained these discrepancies as “process enablers and not errors.” While these errors enable the tech refresh process to proceed, they do not constitute valid Asset Tag numbers or valid computer records in the Asset Center. If erroneous data can be entered to enable a process to continue, then erroneous data can also be entered to conceal theft or mismanagement.

Because their records were not accurate and did not account for all computers, Hewlett-Packard Enterprise Services asset management systems were not able to detect the thefts taking place at either Mechanicsburg or over the 3- to 4-year span at Millington, New Orleans, and other installations. After they were informed of the thefts, Hewlett-Packard Enterprise Services was unable to rely on their records to identify which specific computers had been stolen.

The “Warehouse Operating Procedures Manual” states that “NMCI Asset records exist across Asset Center, the Warehouse Management System, and Financial Accounting Systems. Asset records must be updated and monitored throughout the execution of NMCI Equipment to a warehouse to correctly and methodically account for assets.” Discrepancies and errors of the magnitude found during this audit impede accurate asset accountability and reconciliation. DON tracks its computers through the Enterprise Tool and relies on the accuracy of Asset Center data. DON must have assurance that every computer and hard drive is accounted for to fully safeguard all its information and comply with Secretary of the Navy Instruction 5211.5E. A detailed review of the contractor information systems to determine the exact causes of data inaccuracies was beyond the scope of this audit.

The finding in this report shows the need for more stringent controls to increase accountability. Before the transition to NMCI, laptops, desktops, and printers were accounted for on Naval property records prescribed by Secretary of the Navy Instruction 7320.10A. This regulation requires DON to establish property records and stricter accountability for Government assets that are sensitive or pilferable.²⁷ It also mandates the use of receipt and transfer of custody documentation, bar code marking of assets, and procedures for placing them on property records.

In our opinion, our audit finding, combined with the two investigations in Mechanicsburg and Millington/New Orleans that have occurred after our audit conclusions were formed, provide a basis for concluding that the computer turn-in process is a significant internal control weakness in DON's NMCI asset accountability and management.

Current Initiatives and Future Options

Transitional Activities for Continuity of Services Contract Period. Hewlett-Packard Enterprise Services is preparing to change some of the information systems servicing the contract and the Marine Corps is drafting administrative changes to establish property records for all laptops, desktops, and printers, regardless whether they are Government-owned or leased. When implemented these efforts (shown immediately below), should begin to address the weaknesses identified during the audit. While some corrective actions are already underway, we are making recommendations in this report that will require their implementation to be reported back to us.

- During the Continuity of Services Contract period, Hewlett-Packard Enterprise Services is preparing to phase in a comprehensive Information Technology Service and Asset Management system that will replace the Asset Center, service management, and configuration management applications and other ad hoc databases and tools with an integrated product processing suite. Along with updating their associated business processes, this system is supposed to provide automated discovery of information for the computers and hard drives on, or missing from, the network (such as their unique Asset Tag and serial numbers, and customizable reports), and improve accountability and reconciliation of the asset inventory.
- Headquarters Marine Corps Command, Control, Communications and Computers (C4/CP), with Headquarters Marine Corps Installation and Logistics and Marine Corps Systems Command (PG-10), is drafting a Marine Administrative message to ensure consistent policy and procedures for accountability for laptops, desktops, and printers. When implemented, all these assets, regardless of whether they are Government-owned or leased, will be accounted for in the Defense Property

²⁷Items that have a ready resale value or application to personal possession and that are, therefore, especially subject to theft.

Accountability System and Supported Activities Supply System property custody records. The Marine Corps has issued a contract modification to discontinue the Marine Corps participation in the Continuity of Services contract with Hewlett-Packard Enterprise Services as of 30 September 2011.

Technology solutions such as hands-free mobile devices used in the package delivery industry for scanning, sorting, and routing packages, could be an upgrade to the turn-in, pickup, receiving, and cross-docking processes and improve the overall internal control environment. Incorporating technology is likely to foster standardization, and improve dependability and reliability of the data input to the Asset Center and the Warehouse Management System. When implementing the recommended improvements to the turn-in processes (either as part of the Continuity of Services Contract or another best value option), choosing the best available technology solutions should also be considered.

Recommendations and Corrective Actions

We recommend that the Department of the Navy's Space and Warfare Systems Command Program Executive Office for Enterprise Information Systems:

Recommendation 1. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to match and track all computers for turn-in by both assigned hard drive serial number and computer Asset Tag number.

Recommendation 2. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to develop and implement written standardized operating procedures for pickup of all turned-in computers. Require, at a minimum, verification of Asset Tag data to include assigned hard drive serial number for each computer, and at completion of tech refresh, Hewlett-Packard Enterprise Services provide the contract technical representative an itemized listing that clearly identifies all computers that have been picked up, their assigned hard drives that have been turned over to the activity, and those not picked up. The listing will serve as a transfer of custody document for computers picked up and hard drives left with the activity, signed by the contract technical representative and Hewlett-Packard Enterprise Services representative with a copy sent to the Enterprise Warehouse (in lieu of established end-to-end automated procedures).

Recommendation 3. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to develop and implement written standardized operating procedures for follow up of all tech refresh computers not picked up as scheduled. Require timely, continuous followup with the activity on all

scheduled computers not picked up, identify a specific Hewlett-Packard Enterprise Services individual role and define the responsibilities for that role.

Recommendation 4. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to establish and enforce controls to provide full assurance that all turned in computers have asset identification data completely and accurately recorded in the Asset Center (or its replacement system) database records.

Recommendation 5. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform physical counts of computers received at the cross-dock warehouses and Enterprise Warehouse, match and cross match against signed Seat Deployment Schedule activity listings, Warehouse Management System data, and shipping documentation to clearly identify what was received, shipped, and scanned and what should have been received, shipped, and scanned.

Recommendation 6. For any unmatched physical counts at the cross-dock warehouses and Enterprise Warehouse, choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform a detailed reconciliation for each computer using the Seat Deployment Schedule listing, Warehouse Management System records, and Asset Center (or its replacement system), and record all unaccounted for computers on a Missing, Lost, Stolen, and Damaged report with a copy sent to NMCI Program Manager Office.

Recommendation 7. Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform a comprehensive review of Asset Center records to account for all turned in computers and notify Program Executive Office for Enterprise Information Systems of the review results. Establish a quarterly reconciliation process between the Hewlett-Packard Enterprise Services Asset Center (or its replacement system) and the NMCI Enterprise Tool records, and produce an exception report to identify all records that do not match, and reconcile differences.

The Department of the Navy's Space and Warfare Systems Command Program Executive Office for Enterprise Information Systems did not provide a formal response to the recommendations.

Naval Audit Service comment on the lack of a response to Recommendations 1 through 7. Because the Department of the Navy's Space and Warfare Systems Command Program Executive Office for Enterprise Information Systems did not provide a response to the recommendations, we consider them to be undecided and are resubmitting

them to the Department of the Navy's Space and Warfare Systems Command Program Executive Office for Enterprise Information Systems for a response.

We recommend that the Commander, Navy Cyber Forces:

Recommendation 8. Establish operational instructions and procedures directing how the local commands handle equipment turn-in that shall, at a minimum: require prompt turn in of all computers to the contractor pickup teams, that hard drives are removed, Government personnel to accompany contractor pickup teams, and contract technical representative to maintain custody and status documents; and define roles and responsibilities for followup on computers not picked up after tech refresh.

Recommendation 9. Establish internal controls and provide oversight to ensure compliance with the operational instructions and procedures.

Recommendation 10. Establish internal controls that, as computers transition from Continuity of Services Contract leased to Department of the Navy Government-owned assets, ensure that personal property policy and procedures as required by Secretary of the Navy Instruction 7320.10A are fully implemented to account for all computers.

Commander, Navy Cyber Forces did not provide a formal response to the recommendations.

Naval Audit Service comment on the lack of a response to

Recommendations 8 through 10. Because Commander, Navy Cyber Forces did not provide a response to the recommendations, we consider them to be undecided and are resubmitting them to Commander, Navy Cyber Forces for a response.

We recommend that Commandant of the Marine Corps:

Recommendation 11. As part of the Marine Corps transition from the Continuity of Services Contract, establish operational instructions and procedures directing how the local commands handle equipment turn-in that shall, at a minimum: require prompt turn in of all computers to the Base G6/S6 Asset Manager, and proper procedures are followed for disposal, and that the Asset Manager or Customer Technical Representatives maintain custody and status documents of the hard drives.

Recommendation 12. As part of the Marine Corps transition from the Continuity of Services Contract, establish internal controls and provide oversight to ensure compliance with the operational instructions and procedures.

The Commandant of the Marine Corps did not provide a response to the recommendations.

Naval Audit Service comment on the lack of a response to Recommendations 11 and 12. Because the Marine Corps did not provide a response to the recommendations, we consider them to be undecided and are resubmitting them to the Commandant of the Marine Corps for a response.

Section B:

Status of Recommendations

Recommendations							
Finding ²⁸	Rec. No.	Page No.	Subject	Status ²⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³⁰
1	1	13	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to match and track all computers for turn-in by both assigned hard drive serial number and computer Asset Tag number.	U	Program Executive Office – Enterprise Information Systems	4/18/11	
1	2	13	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to develop and implement written standardized operating procedures for pickup of all turned-in computers. Require, at a minimum, verification of Asset Tag data to include assigned hard drive serial number for each computer, and at completion of tech refresh, Hewlett-Packard Enterprise Services provide the contract technical representative an itemized listing that clearly identifies all computers that have been picked up, their assigned hard drives that have been turned over to the activity, and those not picked up. The listing will serve as a transfer of custody document for computers picked up and hard drives left with the activity, signed by the contract technical representative and Hewlett-Packard Enterprise Services representative with a copy sent to the Enterprise Warehouse (in lieu of established end-to-end automated procedures).	U	Program Executive Office – Enterprise Information Systems	4/18/11	

²⁸ / + = Indicates repeat finding.

²⁹ / 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.

³⁰ If applicable.

SECTION B: STATUS OF RECOMMENDATIONS

Recommendations							
Finding ²⁸	Rec. No.	Page No.	Subject	Status ²⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³⁰
1	3	13	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to develop and implement written standardized operating procedures for follow up of all tech refresh computers not picked up as scheduled. Require timely, continuous followup with the activity on all scheduled computers not picked up, identify a specific Hewlett-Packard Enterprise Services individual role and define the responsibilities for that role.	U	Program Executive Office – Enterprise Information Systems	4/18/11	
1	4	14	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to establish and enforce controls to provide full assurance that all turned in computers have asset identification data completely and accurately recorded in the Asset Center (or its replacement system) database records.	U	Program Executive Office – Enterprise Information Systems	4/18/11	
1	5	14	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform physical counts of computers received at the cross-dock warehouses and Enterprise Warehouse, match and cross match against signed Seat Deployment Schedule activity listings, Warehouse Management System data, and shipping documentation to clearly identify what was received, shipped, and scanned and what should have been received, shipped, and scanned.	U	Program Executive Office – Enterprise Information Systems	4/18/11	

SECTION B: STATUS OF RECOMMENDATIONS

Recommendations							
Finding ²⁸	Rec. No.	Page No.	Subject	Status ²⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³⁰
1	6	14	For any unmatched physical counts at the cross-dock warehouses and Enterprise Warehouse, choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform a detailed reconciliation for each computer using the Seat Deployment Schedule listing, Warehouse Management System records, and Asset Center (or its replacement system), and record all unaccounted for computers on a Missing, Lost, Stolen, and Damaged report with a copy sent to NMCI Program Manager Office.	U	Program Executive Office – Enterprise Information Systems	4/18/11	
1	7	14	Choose the best-value option (Continuity of Services contract modifications/task orders, or other available means) to perform a comprehensive review of Asset Center records to account for all turned in computers and notify Program Executive Office for Enterprise Information Systems of the review results. Establish a quarterly reconciliation process between the Hewlett-Packard Enterprise Services Asset Center (or its replacement system) and the NMCI Enterprise Tool records, and produce an exception report to identify all records that do not match, and reconcile differences.	U	Program Executive Office – Enterprise Information Systems	4/18/11	
1	8	15	Establish operational instructions and procedures directing how the local commands handle equipment turn-in that shall, at a minimum: require prompt turn in of all computers to the contractor pickup teams, that hard drives are removed, Government personnel to accompany contractor pickup teams, and contract technical representative to maintain custody and status documents; and define roles and responsibilities for followup on computers not picked up after tech refresh.	U	Navy Cyber Forces	4/18/11	

SECTION B: STATUS OF RECOMMENDATIONS

Recommendations							
Finding ²⁸	Rec. No.	Page No.	Subject	Status ²⁹	Action Command	Target or Actual Completion Date	Interim Target Completion Date ³⁰
1	9	15	Establish internal controls and provide oversight to ensure compliance with the operational instructions and procedures.	U	Navy Cyber Forces	4/18/11	
1	10	15	Establish internal controls that, as computers transition from Continuity of Services Contract leased to Department of the Navy Government-owned assets, ensure that personal property policy and procedures as required by Secretary of the Navy Instruction 7320.10A are fully implemented to account for all computers.	U	Navy Cyber Forces	4/18/11	
1	11	15	As part of the Marine Corps transition from the Continuity of Services Contract, establish operational instructions and procedures directing how the local commands handle equipment turn-in that shall, at a minimum: require prompt turn in of all computers to the Base G6/S6 Asset Manager, and proper procedures are followed for disposal, and that the Asset Manager or Customer Technical Representatives maintain custody and status documents of the hard drives.	U	Commandant of the Marine Corps	4/18/11	
1	12	15	As part of the Marine Corps transition from the Continuity of Services Contract, establish internal controls and provide oversight to ensure compliance with the operational instructions and procedures.	U	Commandant of the Marine Corps	4/18/11	

Exhibit A:

Background

The Navy/Marine Corps Intranet (NMCI) contract was an indefinite delivery/indefinite quantity firm-fixed-price type contract providing for placement of task orders for various categories of information technology services by Navy and Marine Corps Commands. This type of contract is commonly referred to as “seat management.” Generally speaking, under seat management, contractor-owned desktops and laptops, and other computing hardware, software, and related services are bundled and provided at a fixed price per unit (or seat). Through the NMCI Contract, DON replaced independent local and wide area networks with a single network and related desktop hardware and software that were owned by the contractor.

Every 3 to 4 years each “seat” has its computer and software replaced with updated equipment in a process called “technology refresh” or “tech refresh.” New computers are installed and the old computers are returned to Hewlett-Packard Enterprise Services through the turn-in process for reuse or disposal. The old computers are picked up by a regional cross-dock warehouse for processing to the Enterprise Warehouse in Mechanicsburg, PA.³¹ The computers are scanned into the UniCODE Warehouse Management System by affixed labels with Asset Tag number and serial numbers to record receipt at the cross-dock warehouse and again when they reach the Enterprise Warehouse. The warehouse managers manually make a daily tally of computers picked up and prepare a weekly summary report to Hewlett-Packard Enterprise Services Operations. Once a cross-dock has packed 24 pallets containing 1,056 computers, they are shipped by contract carrier to the Enterprise Warehouse. The tech refresh turn-in process is complete when the computers are received at the Enterprise Warehouse. Sites not served by a regional cross-dock, called “remote sites,” pack up and send their old computers directly to the Enterprise Warehouse. Some of the larger remote sites do establish temporary cross-docks, without Warehouse Management System access, for the duration of their tech refresh.

The current NMCI contract with Hewlett-Packard Enterprise Services expired 30 September 2010. A Continuity of Services Contract was awarded in July 2010 to Hewlett-Packard Enterprise Services to transition NMCI to the Next Generation Enterprise Network (NGEN). The Continuity of Services Contract is an indefinite delivery/indefinite quantity fixed-price with award fee type contract providing for placement of task orders for various categories of information technology services by

³¹Cross-dock warehouses only pick up, palletize, and ship turned in computers. Permanent cross-dock warehouses are located at Andrews Air Force Base, MD; Patuxent River Naval Air Station, MD; St. Juliens Creek, VA; Camp Lejeune Marine Corps Base, NC; Naval Station Bremerton, WA; San Diego, CA; Camp Pendleton Marine Corps Base, CA; Ford Island, HI; and Okinawa, Japan. The Enterprise Warehouse is in Mechanicsburg, PA and receives, stores, sanitizes, and disposes of refreshed computers.

Navy and Marine Corps Commands. During the period of performance of this contract, DON will transition from receiving materials and services outlined in this statement of work from the contractor to ultimately receiving no services under this contract. At the conclusion of this contract, DON will have transitioned information technology services, materials, and capabilities in seven service areas provided under the NMCI Continuity of Services Contract to the NGEN system provided by the Government or another contract.

Exhibit B:

Pertinent Guidance

Secretary of the Navy Instruction 5211.5E, “Department of the Navy Privacy Program,” 28 December 2005, states that DON activities shall establish appropriate administrative, technical, and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected.

Secretary of the Navy Instruction 5239.3A, “Department of the Navy Information Assurance Policy,” 20 December 2004, establishes within DON an Information Assurance policy that provides information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access to, use, disclosure, disruption, modification, or destruction of (1) Information collected or maintained by or on behalf of DON; and (2) Information Systems used or operated by DON, by a contractor of DON processing DON information, or other organizations on behalf of DON.

Secretary of the Navy Instruction 7320.10A, “Department of the Navy (DON) Personal Property Policies and Procedures,” 1 April 2004, establishes DON policies and procedures for personal property management. Accountable records shall be established and maintained in a compliant personal property system for all personal property purchased, leased (capital or operating leases as applicable), or otherwise obtained, having a unit acquisition cost of \$5,000 or more, as well as items that are below \$5,000 and are sensitive, classified, or meet all of the following three criteria: (1) pilferable; (2) critical to the activity’s business/mission; and (3) hard to repair or replace. Additional and/or separate records or other record keeping instruments shall be established for management purposes when a risk assessment indicates the need for more stringent controls, or when otherwise required by law, policy, regulation, or Agency direction.

Secretary of the Navy M-5239.1, “Department of the Navy Information Assurance Program Manual,” November 2005, requires the protection of all electronic media (e.g., compact disks, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information from unauthorized access; and control of access to such materials; and ensure they are properly labeled, stored, destroyed, and disposed of in accordance with the rules for the data they contain including all sensitive unclassified data not approved for public release.

Navy/Marine Corps Intranet (NMCI) Contract N00024-00-D-6000, Attachment 1 – Statement of Objectives (7 April 2006); and Attachment 4 – Security Requirements (6 October 2000), requires the contractor to develop procedures and implementation plans to ensure that information technology resources leaving the control of the assigned

user are cleared of all DON data and sensitive application software by a technique approved by the Government.

Marine Administrative 318/03 NMCI Transition Warning Order Transition Message No. A003, 3 July 2003, requires Commandant of the Marine Corps to ensure that commands/activities understand that Electronic Data Systems (EDS)³² will assume accountability and support responsibility for a Command's/activity's Information Technology/Automatic Data Processing Equipment (IT/ADPE) assets through transition to NMCI-EDS; which includes EDS replacing currently used IT/ADPE assets with new EDS-furnished assets. Commands/activities shall remove IT/ADPE assets from their property accountability records. IT/ADPE assets, regardless of whether they are privately owned, owned by the Government, or Electronic Data Systems, are classified as pilferable items subject to Missing, Lost, Stolen, Recovered procedures.

Chief of Naval Operations Message 261536Z OCT 01, Subj/Navy Marine Corps Intranet (NMCI) Automated Data Processing Equipment (ADP) Turnover Process, 26 October 2001, provides guidance to all DON activities concerning the subject process in order to ensure accurate identification of all DON-owned automated data processing assets turned over to NMCI contractors. Property management policy is straight forward: if the asset is labeled as an Electronic Data Systems asset, it will be removed from Navy property records.

NMCI Continuity of Services Contract N00039-10-D-0010, Attachment 1 – Statement of Work, 1 July 2010, describes the work required to be performed by the contractor under this Continuity of Services Contract. For example: it requires the contractor to develop procedures and implementation plans to ensure that information technology resources leaving the control of the assigned user are cleared of all DON data and sensitive application software by a technique approved by the Government; and requires the contractor to track all Contractor Furnished Equipment and Government Furnished Equipment Information Technology assets with a purchase price in excess of \$250, except cable plant, supporting the network in accordance with Department of Defense Instruction(s) 5000.64, 4165.14, and 4140.1-R; and Department of Defense 4000.25-2-M, Federal Acquisition Regulation Part 45.000, and Secretary of the Navy Instruction 7320.10A.

³² Now Hewlett-Packard Enterprise Services.

Exhibit C:

Scope and Methodology

Scope

The audit team conducted an audit of the Navy/Marine Corps Intranet (NMCI) tech refresh turn-in process between 15 January 2009 and 15 February 2011. Our audit work focused on the NMCI turn-in process for unclassified computers. The process is managed by Hewlett-Packard Enterprise Services. Specifically, we analyzed data from four Hewlett-Packard Enterprise Services databases and one Department of the Navy (DON) database for the period of 31 March 2008 through 1 May 2009 that track computers throughout the tech refresh turn-in process. During this scope period, there were 17 claimants (16 Navy plus the Marine Corps) that received tech refresh computers, comprised of 804 Unit Identification Codes, with a total of 99,791 unclassified computers (figures derived from NMCI Enterprise Program Office reports - EPM Actual Cutover).³³ There were nine permanent Hewlett-Packard Enterprise Services cross-dock warehouses used to store turned in computers en route to the Enterprise Warehouse in Mechanicsburg, PA.

This audit followed our audit “Processing of Computers and Hard Drives During the Navy/Marine Corps Intranet (NMCI) Computer Disposal Process” N2009-0027, 28 April 2009. Due to significant internal control deficiencies found in the disposal process, the turn-in issue was identified and developed as a separate, additional audit topic. There were no previous reports of the NMCI tech refresh turn-in process on which to follow up.

Methodology

We interviewed key DON personnel in the Program Executive Office – Enterprise Information Systems, the NMCI Program Management Office, and Hewlett-Packard Enterprise Services and their subcontractors. We interviewed DON Contract Technical Representatives, Assistant Contract Technical Representatives, and personnel with tech refresh duties, as well as management officials and warehouse personnel from Hewlett-Packard Enterprise Systems and their subcontractors.

We reviewed compliance with contract and procedural guidance, policy, laws, and regulations applicable to the tech refresh turn-in process for NMCI computers.

³³“Cutover” is the NMCI term for Hewlett-Packard Enterprise Services making a seat operational for the user. In this case, this is the report for completed Tech Refreshes.

We sent an automated survey questionnaire to tech refresh experts at 16 Navy claimants and the Marine Corps³⁴ to collect information and assess potential risk areas.

We visited activities and warehouses to assess that internal control were sufficient to safeguard computers with DON official information and personally identifiable information from loss or theft.

We selected site locations to observe tech refreshes based on the schedule published in the NMCI Homeport web site and adjustments made to that schedule. We physically observed the tech refresh turn-in process at the following four Navy and Marine Corps Commands:

- Marine Corps Combat Development Command, Quantico, VA
- Commander, Naval Installations Command, Norfolk Naval Station, Portsmouth, VA
- Marine Corps Institute, Washington Navy Yard, DC
- Naval Sea Systems Command, Washington Navy Yard, DC

We interviewed warehouse personnel and observed warehouse procedures at three of the nine cross-dock warehouses (refer to Exhibit D for activities visited) and the Enterprise Warehouse in Mechanicsburg, PA. We conducted these visits in conjunction with the Command site visits to assess controls and track the computers from the activities to the Enterprise Warehouse.

In cooperation with the Naval Audit Service Data Analysis Division and Statistician, we performed various tests of the four Hewlett-Packard Enterprise Systems databases/information systems (Asset Center, Warehouse Management System, Seat Deployment Schedule Pick Up Reports, and Order Installation and Confirmation Deployment) and the DON NMCI Enterprise Tool database to assess data reliability. The “Asset Tag number” data field was the primary unique identifier for all tests because each computer is assigned a unique 10 digit Asset Tag number and this data field appears in all the databases we used. We conducted tests for duplicate/repeat entries; erroneous or suspicious Asset Tag numbers; and queries between databases to identify mismatched entries. We also compared data between databases to track and account for computers throughout the tech refresh turn-in process. We did not test the reliability of the data because such tests would have constituted a significant audit effort that was outside the scope of our audit.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the

³⁴We selected survey recipients based on their having either undergone or scheduled for an impending tech refresh during our scope period.

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.

Communication with Management. Throughout the audit, we kept the NMCI Program Management Office and contractor informed of the audit progress. Specifically, we held bi-weekly teleconference meetings with contractor, and NMCI Program Management Office representatives to discuss our progress, next steps, required official documents, and management responses by the contractor to address policy, procedure and data analysis questions. As we entered the report writing phase, we maintained regular contact with the NMCI Program Management Office representatives via meetings, phone calls and emails discussing audit progress, issues related to the Continuity of Services Contract, and the theft incidents.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal Agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1-12 address issues related to internal controls over the NMCI turn-in process. In our opinion, the weaknesses noted 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

Program Executive Office for Enterprise Information Systems, Arlington, VA*

NMCI Program Office, Arlington, VA*

Cross-dock warehouse, Andrews Air Force Base, Suitland, MD*

Cross-dock warehouse, St. Juliens Creek, Portsmouth, VA*

Cross-dock warehouse, Patuxent River Naval Air Station, Patuxent River, MD*

Cross-dock warehouse, Camp Lejeune Marine Corps Base, NC

Cross-dock warehouse, Naval Station Bremerton, WA

Cross-dock warehouse, Camp Pendleton Marine Corps Base, CA

Cross-dock warehouse, San Diego, CA

Enterprise Warehouse, Naval Supply Systems Command (NAVSUP), Naval Inventory Control Point, Mechanicsburg, PA*

Norfolk Naval Station, Norfolk, VA*

Marine Corps Combat Development Command, Quantico, VA*

Naval Sea Systems Command, Washington Navy Yard, Washington, DC*

Marine Corps Institute, Washington Navy Yard, Washington, DC*

Navy/Marine Corps Intranet Enterprise Tool Office, Alexandria, VA*

Hewlett-Packard Enterprise Services (formerly Electronic Data Systems), Herndon, VA*

* Indicates visit made by audit team

We distributed the survey questionnaire to several commands:

Department of the Navy, Assistant for Administration
Military Sealift Command
Chief of Naval Operations
Commander, United States Pacific Fleet
Bureau of Naval Personnel
Naval Sea Systems Command
Space and Naval Warfare Systems Command
Naval Supply Systems Command
Naval Air Systems Command
Naval Facilities Engineering Command
Headquarters Marine Corps
Marine Corps Training and Education Commands
Marine Corps Systems Command
Marine Forces Command
Marine Forces Pacific
Marine Forces Reserve
U.S. Fleet Forces Command
Navy Reserve Force
Commander, Navy Installations Command

Exhibit E:

Survey Comments

In response to our Survey Questionnaire question seeking suggestions for improvements, we received the following comments addressing internal control issues with hard drives, pickup procedures, and followup procedures:³⁵

Hard Drives

- Provide “formal and all-inclusive documentation that tracks delivery of tech refresh, pick up of outgoing assets, receipt of outgoing asset by warehouse, validation and sign off that all Government data removed from all outgoing unclassified hard drives, validation and custody transfer of all NNPI (Naval Nuclear Propulsion Information) and Classified hard drives.”
- Provide an “online tool that can be accessed by both the Navy and the contractor; such as, barcode location program similar to the UPS or FedEx system.”

Pickup Procedures

- “EDS (Electronic Data Systems) needs to have a solid pick up program on file and follow the program completely.”
- “Clarify what is supposed to happen and provide instructions.”
- “Standardize tech refresh pick up process and documentation for all sites.”
- “Unfortunately there is no supporting documentation on equipment being returned to EDS.”
- “Contractor could give receipts to Command when picked up.”
- “Upon picking up assets EDS/HP (Hewlett-Packard) should provide Commands with a receipt.”

³⁵Comments edited for grammar.

- “EDS needs to incorporate into their tech refresh process procedures for receiving NMCI (Navy-Marine Corps Intranet) seats and pick up of retired assets.”
- “Confirmation of delivery to the warehouse of all assets and signed documentation would be useful.”
- “Instruct the NMCI Contractor to provide the government a listing of returned computers as this is not their routine.”
- “Written acceptance from warehouse personnel of retired assets.”
- “Provide documents of outgoing computers received in their custody.”
- “Once the replacement was received, there was no accountability for retrieving the old asset.”
- “Suggested improvements such as deliverables to the Government, for example, a report of assets delivered to the specific delivery points and a report of assets picked up by the EDS/NMCI logistics team, signed by the NMCI logistics team after verification by the Government.”
- “Records and accountability for assets is terrible. Site Manager will tell me I owe him assets, Marines say it was picked up...what do I do? Delivery people are going through squadrons without escorts and rummaging through things looking for NMCI machines. This is inappropriate.”
- “Provide a list to the Command of returned computers at the end of tech refresh. If 200 computers were refreshed, then 200 computers should be picked up.”
- “It is a little late but having accountability for inventory that NMCI picked up would have been helpful. In a way this was being done. NMCI would not drop off a new asset unless they verified the outgoing asset. However, we never received a signed receipt from NMCI.”
- “The Government should consider incorporating into the NMCI contract a deliverable requirement for a final report from EDS that certifies to receipt and final disposition of all tech refresh assets according to all applicable Government laws and policy.”
- “EDS needs to track the pickups better, since they have the contractual obligation to pick up the assets in a timely manner as defined by any existing business rule.”

Perhaps EDS can provide a drop off location so the Government can be held harmless for these retired assets.”

- “Prompt pick up in accordance with Execution Discipline” should be exercised. Commands would like “documentation provided to confirm old asset was picked up and has been received by the warehouse. Written acceptance from warehouse personnel of retired assets” is appreciated.
- “I noticed a couple of times, the TR (tech refresh) deployer took a retired asset without looking at the asset number on the computer. I would have thought they would have looked at the asset number to confirm that it was definitely an asset that should have been taken.”
- “Ensure NMCI Enterprise Tool works. Specifically when computers are placed in a build out for refresh and an error occurs, the error should get fixed immediately instead when refresh occurs, which causes a delay in refresh some computers.”

Followup Procedures

- “Alternatives for assets that are not picked up in a timely manner; such as seats will be stored at EDS Site Ops on base until the EDS Logistics Team can pick them up.”
- “I asked the TR (tech refresh)Deployment Lead for a list of retired assets that had been picked up to date so that we could determine which asset still remained; we were never given that document. So the responsibility fell back on the ACTR (Assistant Contract Technical Representative) to determine which retired assets were still outstanding.”
- “It was painful getting our retired assets picked up. The ACTR (Assistant Contract Technical Representative) sent out emails to all Departments on base to find out who still had retired assets that had not been picked up after TR (tech refresh). We were shocked to find there were a lot still scattered around the base. The Government should have been provided a list of the retired assets that were picked up so we knew which assets still needed to be removed.”
- “We always meet with the warehouse personnel for delivery of the new assets but have had no involvement for pickup of the old assets. I never knew there was an actual process in place. At times I had to send NMCI (EDS) an email telling them about assets not picked up from a refresh conducted months earlier.”

In response to our Survey Questionnaire question seeking suggestions for improvements, we also received the following positive comments:

- “Our NMCI asset turn-in was handled in an effective and timely fashion. Unfortunately there is no supporting documentation on equipment being returned to EDS. Note: EDS has full ownership of *ALL* NMCI equipment.”
- “It’s been working.”
- “Our tech refresh went smoothly.”
- “Things went pretty smoothly; no problems that I know of.”
- “OUTSTANDING!”

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies
of this document

~~FOR OFFICIAL USE ONLY~~