

# Naval Audit Service



## Audit Report



# Processing of Computers and Hard Drives During the Navy Marine Corps Intranet (NMCI) Computer Disposal Process

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

~~Releasable outside the Department of the Navy~~  
~~only on approval of the Auditor General of the Navy~~

N2009-0027  
28 April 2009

## 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](mailto: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

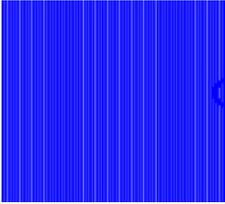
To suggest ideas for or to request future audits, please use the following contact information:

**Phone:** (202) 433-5840 (DSN 288)  
**Fax:** (202) 433-5921  
**E-mail:** [NAVAUDSVC.AuditPlan@navy.mil](mailto: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/navalauditservices>



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

7510  
 N2008-NFO000-0025.001  
 28 Apr 09

MEMORANDUM FOR DISTRIBUTION

**Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (AUDIT REPORT N2009-0027)**

**Ref:** (a) NAVAUDSVC Memorandum 7510 N2008-NFO000-0025, dated 16 Nov 07  
 (b) SECNAVINST 7510.7F, "Department of the Navy Internal Audit"

- Encl:** (1) Status of Recommendations  
 (2) Scope and Methodology  
 (3) Pertinent Guidance  
 (4) Auditor General Alert of 25 February 2008  
 (5) Management Response from Department of the Navy Chief Information Officer and Assistant Secretary of the Navy (Research, Development, and Acquisition)  
 (6) Management Response from Commandant of the Marine Corps  
 (7) Management Response from Commander, Naval Network Warfare Command  
 (8) Management Response from Program Executive Officer (Enterprise Information Systems)

1. We have completed the subject audit, announced by reference (a) and are providing this final report for your review in accordance with reference (b). The table below notes the action command for each recommendation.

Command	Finding No.	Recommendation No.
Department of the Navy Chief Information Officer	1	1-4
Naval Network Warfare Command	1	5-8
Commandant of the Marine Corps	1	9-12
Program Executive Office – Enterprise Information Systems	1	13-14
Assistant Secretary of the Navy (Research, Development and Acquisition)	1	15

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**2. Summary.**

a. Department of the Navy (DON) hard drives containing “Secret” and/or personally identifiable information (PII)<sup>1</sup> were improperly stored at two warehouses used by Electronic Data Systems Corporation (EDS), the contractor that supports the Navy Marine Corps Intranet (NMCI). Some of the hard drives contained both classified information and PII, were not properly secured, and were readable with commercially available recovery software. Most of the hard drives containing classified information had been certified by Government officials as having been degaussed (rendered inoperable), though some could still be read. The hard drives containing PII were operable and accessible, even though EDS personnel had previously certified they were inoperable. Using discovery sampling, auditors also found a computer ready for sale to the public that still contained DON data and PII (including 605 unique Social Security numbers (SSNs)) at one of the warehouses. Notably, the computer had twice been certified by EDS personnel as having been properly cleared of all DON data. Had DON and EDS not changed processing procedures to address our findings early in the audit, we statistically project that over a thousand more computers containing DON data and/or PII could have been made available to the public in calendar year 2008 (see “Findings” for details). DON policies require the proper safeguarding and disposal of classified information, official DON data, and PII. However, because these policies were not effectively implemented, and in some areas were not sufficient, sensitive data was not properly safeguarded and/or disposed of, and was easily accessible using commercially available software. Unauthorized access to classified and sensitive DON information poses a national security risk, and unauthorized access to PII increases the risks of identity theft for DON military and civilian personnel. Both situations bring a significant risk of embarrassment to DON. Strengthening policies and procedures over the disposal process, including, but not limited to, requiring the physical destruction of all hard drives being removed from DON control will help mitigate these risks.

b. We worked closely with the Program Executive Officer (Enterprise Information Systems) (PEO-EIS) and his staff throughout the audit. We provided them with our observations, findings, suggestions, and recommendations on a real-time basis. In response, the PEO-EIS quickly took a number of corrective actions while the audit was still ongoing. For example, in February 2008, we provided PEO-EIS with a draft Auditor General Alert (Enclosure 4) which suggested, among other things, that the PEO-EIS impose a DON-wide moratorium on the release to the public of DON computers containing hard drives, pending a review of EDS’ disposal process. The PEO-EIS implemented the moratorium, and, during the course of the audit, also issued two Operations Event/Incident Report (OPREP-3) Navy Blue memos. OPREP-3 Navy Blue

---

<sup>1</sup> We identified 14 hard drives containing accessible classified information; we also identified 23 hard drives containing readily accessible Social Security numbers, and project that an additional 612 hard drives contained readily accessible Social Security numbers (see “Findings” for details).

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

memos are operational reports on issues<sup>2</sup> of high Navy interest that notify Navy senior leaders of conditions and actions taken and planned. Related OPREP-3 Navy Blue memos made senior DON leaders aware of our specific audit observations and findings, and the actions PEO-EIS had taken or planned to take to address them. Also, as a result of the increased attention brought to these issues by the audit; EDS discovered and self-reported 4 additional incidents involving 24 different classified hard drives, which led to 4 more OPREP messages. Additionally, on 29 August 2008, we provided the PEO-EIS with six preliminary audit recommendations. Although audit work was still ongoing, as of September 2008, our preliminary audit work (which we briefed to NMCI management on a frequent and ongoing basis) led to EDS assigning a fulltime onsite manager to oversee the disposal process, and to the PEO-EIS and EDS making plans and initiating actions to improve policy governing the: (1) handling, disposition, and transport of classified materials; (2) tracking of separated hard drives; (3) maintenance of separate disposal streams for classified and unclassified hard drives; (4) timeliness of disposal of hard drives; and (5) restructuring of disposal processing procedures.

c. In December 2008, Naval Network Warfare Command (NETWARCOM) issued a Navy Telecommunications Directive establishing policy<sup>3</sup> that requires the physical destruction of hard drives with classified and controlled unclassified information used by the Naval Criminal Investigative Service (NCIS) and select communities. We support the requirement to physically destroy hard drives, and recommended hard drive destruction to the PEO-EIS in August 2008. However, we concluded that *all* DON hard drives, not just hard drives with classified and controlled unclassified information from select communities, and not just those in NMCI computers, should be physically destroyed when removed from DON control. Physically destroying all DON hard drives should significantly reduce the possibility of human or technical errors, such as those that allowed hard drives incorrectly believed to have been cleared of sensitive DON data or degaussed, to enter unsecure waste streams, and/or be available for release to the public while still containing readily accessible sensitive data. We formally make the recommendation in this report to destroy all NMCI and non-NMCI hard drives. This recommendation, and our related recommendations to improve the existing NMCI and future Next Generation Enterprise Network (NGEN) computer disposal processes, are in Paragraph 5, "Recommendations and Corrective Actions."

d. The Navy Telecommunications Directive cited in the prior paragraph notes recent events (such as those found during this audit) as evidence of need for improvement, and indicates that commands will be subject to oversight by the Naval Audit Service and others. Also, during our Fiscal Year 2009 annual audit planning process, the Director, Navy Staff indicated that safeguarding all DON data was a priority, and requested that

---

<sup>2</sup> An OPREP-3 Navy Blue memos address "spill" issues. Spill issues refer to a leak of military resources, and may be chemical or electronic spillages.

<sup>3</sup> This was initially issued as interim policy in November 2008.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

the Naval Audit Service continue to provide audit oversight for the foreseeable future.

e. **Noteworthy Accomplishments.** On 27 April 2009, DON CIO responded to this report by saying “The cost of physically destroying all hard drives (less those sent to NSA) is an unfunded requirement, but the benefits to DON outweigh those costs by ensuring no classified information or sensitive but unclassified information, including personally identifiable information (PII) is compromised. The cost of data spillages and PII breaches is incalculable and negatively impacts our personnel, stresses already constrained command resources and tarnishes our public image with the perception that our data is not properly safeguarded. We cannot continue with a policy that mitigates the risk but rather, we must implement and enforce a strict disposal/redistribution process with proper controls in place to ensure, with complete accuracy and timeliness, that all hard drives are physically destroyed. This risk avoidance policy will apply to all hard drives and all external media with memory, including servers, routers, switches and external portable hard drives no longer under government control.” This response goes beyond the recommendations in this report. By applying our findings and recommendations to all external media with memory, DON CIO will further reduce the risk of unauthorized access to classified and sensitive DON information and PII.

### 3. **Reason for Audit.**

a. Our objective was to verify that internal controls over the NMCI disposal process were sufficient to protect DON and personal data. The audit was self-initiated by the Naval Audit Service and approved by the Oversight Planning Board.

b. The audit focused on NMCI’s disposal of unclassified DON computers and computer hard drives during the tech-refresh process (the periodic upgrade of existing NMCI workstations with new hardware to provide increased technological capabilities and performance for NMCI users). The disposal of classified computers and classified hard drives was not the initial focus of this audit; however, testing to verify that the unclassified hard drive disposal stream did not contain classified hard drives was part of this audit effort. Audit work was primarily conducted from November 2007 to March 2009. On-site testing, analysis, and inventorying was done at the three main warehouses<sup>4</sup> used by EDS in the final processing of computers turned in as part of the NMCI “tech-refresh” process, and at subcontractor facilities that handled final disposition (e.g., sale, donation, or destruction) of computers and hard drives.

---

<sup>4</sup> NMCI processed computers at warehouses located in Mechanicsburg, PA; San Diego, CA; and Ford Island, HI. Scrubbing operations (clearing hard drives of data) at San Diego, CA and Ford Island, HI were discontinued in February 2008 and September 2007 respectively. All scrubbing is now done at the Mechanicsburg, PA warehouse.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**4. Results.**

**a. Classified Hard Drives and Accessible PII**

(1) **Classified Hard Drives.** We found hard drives marked with the “Secret” designation sticker in a large shipping container mixed with unclassified hard drives containing PII. Because the container was located in an open area at the Ford Island, HI, warehouse used by EDS, we notified PEO-EIS staff, EDS site management, and NCIS. Analysis of these and other classified hard drives from the Ford Island warehouse revealed that 14 of the 114 testable hard drives contained accessible classified information. Of these, 12 had been certified as having been degaussed and, therefore, should not have been operable or contained any data. Secretary of the Navy M-5510-36, “Department of the Navy Information Security Program” (June 2006), requires that classified material be stored in a locked General Services Administration-approved security container, vault, modular vault, or secure room. Details follow.

(a) At the Ford Island facility, on 16 April 2008, auditors found 2,050 hard drives in a container<sup>5</sup> in an unsecured area accessible to staff not holding proper security clearances. The auditors identified 4 hard drives with full red “Secret” stickers (SF-707) and 96 with remnants of the sticker or a sticker marked through with a black marker.<sup>6</sup> Using commercially available software, the audit team was able to test<sup>7</sup> 74 of the 100 stickered hard drives.<sup>8</sup> Five hard drives were found to contain data classified as “Secret.” We were able to verify, by matching hard drive serial numbers to documents discovered on-site at the warehouse,<sup>9</sup> that three of five hard drives had been certified by a Government official as having been degaussed. EDS later shipped these hard drives from Ford Island to the Mechanicsburg, PA warehouse for further processing.

---

<sup>5</sup> Commonly referred to as a “Gaylord” box.

<sup>6</sup> An NCIS agent met with the auditors on site and advised EDS personnel on proper methods of securing the hard drives.

<sup>7</sup> On 21 April 2008, we shipped the 100 hard drives to our office at the Washington Navy Yard and tested them there.

<sup>8</sup> 26 of 100 were not tested due to damage to pins or other hard drive components.

<sup>9</sup> The team found some of the documents attached to, or inside boxes, while others were given to us by an EDS employee.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (AUDIT REPORT N2009-0027)**



Above left shows hard drives in a container at the Ford Island warehouse. Above right are examples of hard drives with intact “Secret” stickers found, mixed with unclassified hard drives, in the container.

(b) At the Mechanicsburg warehouse, on 28-29 July 2008, auditors conducted a 100 percent inventory of the container of hard drives that had been shipped from Ford Island<sup>10</sup> to Mechanicsburg for disposal processing. The inventory showed that more hard drives had been shipped from Ford Island than were originally identified by the auditors while at Ford Island. EDS acknowledged that approximately 400 (399 per our inventory) additional hard drives had been found in a different part of the Ford Island warehouse after the auditors left the site, and, therefore, were included in the hard drive shipment to Mechanicsburg. Of the 2,449 (2,050 plus 399) hard drives from Ford Island, the auditors identified<sup>11</sup> and tested 40 additional classified hard drives. The tests showed that nine of these hard drives were operational and contained easily accessible information classified as “Secret.” None of these hard drives contained appropriate classification markings.

(c) We were unable to determine why classified hard drives were mixed in a container with unclassified hard drives, and why some had been certified as having been degaussed when they had not been.

## (2) Accessible PII (SSNs)

(a) We also found unclassified hard drives that had not been cleared of all DON data (including PII) in an open, unsecured area of EDS’ Ford Island warehouse. Secretary of the Navy Instruction 5211.5E, DON Privacy Program, 28 December 2005, requires that safeguards be in place to protect the confidentiality of PII.

<sup>10</sup> The hard drives were shipped from Ford Island to Mechanicsburg on 23 April 2008.

<sup>11</sup> We identified the hard drives as classified hard drives by matching either serial numbers or computer names to degaussing documents that had been prepared by the commands submitting the drives, and which we found at the warehouse.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

(b) On 18 April 2008, we arbitrarily pulled three hard drives with no classification markings from the container of 2,050 hard drives at the Ford Island warehouse. We shipped the three hard drives to our office at the Washington Navy Yard for examination, and determined that all three contained SSNs.<sup>12</sup> We arbitrarily selected and examined an additional eight unmarked hard drives from the box after it had been shipped to Mechanicsburg, PA. We were able to easily access information on the hard drives, which should have been inoperable, again using commercially available software. Five of the eight drives contained For Official Use Only (FOUO) information and/or PII (including SSNs). To determine the magnitude of the situation, we statistically sampled 60 of the 2,449 hard drives now located at the Mechanicsburg warehouse. Of the 60, we found that 15 contained readily accessible SSNs. Based on our sample results, we can statistically project that 612 of the 2,449 hard drives were operable and contained in excess of 5,000 documents with SSNs. Many of the documents contained multiple SSNs. The hard drives also contained other PII, such as names, addresses, ranks, phone numbers, banking information, and documents with FOUO statements.

(c) We were unable to determine why operable unclassified hard drives were being stored at Ford Island, and why they still contained PII and other DON data.

**(3) Hard Drive Management Observations.**

(a) **Timely Disposition of Hard Drives.** We found that there was no NMCI guidance that addressed or required the timely disposition of hard drives entered into the disposal process. The Ford Island warehouse manager did not know how long the hard drives had been improperly stored in the container at the warehouse. He speculated that the drives had been collected for over a year, but did not know why they were collected and stored, or why they had not yet been shipped to the Mechanicsburg warehouse. Because hard drives were not inventoried and tracked (see below), we were not able to determine when they had arrived at Ford Island and, thus, how long they had been there. We did note, however, that the data on some of the hard drives was dated no later than 2002 – indicating that those hard drives may have been out of use and could have been at the Ford Island warehouse for 5 or 6 years. Not requiring the timely disposal of hard drives increases the window of opportunity for hard drives containing DON data to be inappropriately accessed.

(b) **Tracking of Hard Drives.** There was no DON or EDS centralized tracking system for hard drives.<sup>13</sup> EDS assigns every computer an asset number and a service tag/serial number. However, EDS does not assign an identifying number to the

---

<sup>12</sup> SSNs are considered a “high-risk” factor according to the Risk Assessment Model in the OSD Memorandum on Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 21 September 2007.

<sup>13</sup> Some local commands included hard drive serial numbers on the degaussing documentation. However, this was not a consistent or centralized practice.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

hard drive within the computer, or record the manufacturer type serial numbers found on the hard drives. Thus, when hard drives are separated from computer shells, as was the case for the 2,050 hard drives discussed above, one can not determine from which computers the separated hard drives came. Without this information, DON can have no assurance that all separated hard drives are properly disposed of. Because of this lack of inventory control, DON cannot know if hard drives with classified and/or sensitive data and PII are lost or stolen. As a result, personal identities and national security could be compromised without DON's knowledge.

(4) **Transition to NGEN.** NGEN is intended to replace NMCI. Department of the Navy Chief Information Officer (DON CIO) is responsible for developing the vision, strategy and concept of operations for NGEN. PEO-EIS is responsible for contracting for NGEN. While we did not address specific NGEN plans during this audit, it is imperative that internal controls to prevent the recurrence of the kind of problems we found during this audit be incorporated into NGEN policies, procedures, and governance practices.

(5) **Cost vs. Benefit of Physically Destroying Hard Drives.** Physically destroying all hard drives may be expensive, and will require a significant change in controls and practices. However, the unintended release of DON data could also be very costly to DON and its personnel. For example, significant costs could be associated with mitigating the impacts of security breaches and also with notifying individuals of potential PII compromises.<sup>14</sup> Additionally, and perhaps equally important, but not necessarily quantifiable, is the negative impact a breach could have on national security, DON's and the Government's reputation, and an individual whose identity has been stolen.

## 5. Recommendations and Corrective Actions.

We recommend that Department of the Navy Chief Information Officer:

**Recommendation 1.** Develop policy that requires the timely and permanent *physical* destruction of *all* DON classified and unclassified hard drives (NMCI and non-NMCI) prior to the drives being removed from DON control (except for those being sent to the National Security Agency (NSA) for destruction in accordance with NETWARCOM Telecommunication Directive of 12/08). For hard drives not sent to NSA for destruction, the method(s) of destruction must physically destroy the hard drive (i.e., shredding or crushing the hard drive itself vs. only degaussing to destroy the data) and all data on it. The destruction method(s) identified in the DON CIO policy must provide 100 percent assurance

---

<sup>14</sup> In 2006, an employee of the Veterans Administration lost a laptop, containing the Social Security numbers of up to 26.5 million veterans and active-duty troops. This loss resulted in a law suit by veterans groups, which reportedly cost the Government \$20 million to settle. Another area of monetary loss to the Government is time spent notifying victims of possible breaches of security.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

that physically destroyed DON hard drives cannot later be made operational, and/or their data accessible.

**Management response to Recommendation 1.** Concur. The cost of physically destroying all hard drives (less those sent to NSA) is an unfunded requirement, but the benefits to DON outweigh those costs by ensuring no classified information or sensitive but unclassified information, including personally identifiable information (PII), is compromised. The cost of data spillages and PII breaches is incalculable and negatively impacts our personnel, stresses already constrained command resources and tarnishes our public image with the perception that our data is not properly safeguarded. We cannot continue with a policy that mitigates the risk but rather, we must implement and enforce a strict disposal/redistribution process with proper controls in place to ensure, with complete accuracy and timeliness, that all hard drives are physically destroyed. This risk avoidance policy will apply to all hard drives and all external media with memory, including servers, routers, switches and external portable hard drives no longer under government control.

DON Policy will be developed within 90 days of the date of this memorandum. However, DON CIO will submit an update no later than 20 June 2009.

**Naval Audit Service comment on response to Recommendation 1.** Actions planned meet the intent of the recommendation. Though DON CIO states that they will develop the necessary policy in 90 days, in Recommendation 4, they state that they plan to have the recommendations implemented within 6 months of their management response letter. The interim target date will be 20 June 2009, and the final target completion date will be 30 October 2009.

The Commandant of the Marine Corps provided comments on Recommendation 1, which was addressed to DON-CIO. Specifically, the Commandant suggested that there be a “modification of the recommendation to identify a specific time period for destruction of hard drives; as written, use of the word “timely” is subjective.” We appreciate the Commandant’s comment and agree that a specific time period for destruction would be beneficial. We encourage the Marine Corps to address this issue with DON CIO as the new DON policy is developed.

The Program Executive Office (Enterprise Information Systems) (PEO-EIS) also commented on Recommendation 1. PEO-EIS stated that “While Recommendation 1 would provide a more final solution to the potential loss of PII during the NMCI technical refresh process, PMW-200 is concerned with

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

the unfunded cost associated with such a policy.” We note that ASN (RD&A)’s response to Recommendation 15 states they will identify the necessary funds. Therefore, while we note PEO-EIS’ concern, we accept ASN (RD&A)’s commitment to making funds available for DON to avoid the risks identified in this report.

PEO-EIS also expressed concern about the destruction of hard drives being redundant to other steps NMCI is taking to secure hard drives while in use (the Data at Rest program). We recognize the value of the Data at Rest program. However, given the significant and multiple data safeguarding failures found during the audit, we concluded that the destruction of all hard drives is necessary to minimize risk to national security and individuals. It is important to note that the risk of one exposure can be great, as evidenced by the result of the loss of a laptop by the Veteran’s Administration, and that the risk of human error will always be present. Destroying the hard drives reduces the risk of human error that we found did occur in significant ways in the current hard drive disposal process.

**Recommendation 2.** Develop policy that requires all user organizations to ensure the removal of hard drives (classified and unclassified) from computers that will no longer be subject to DON control, and to ensure the hard drives are properly secured until they can be physically destroyed in accordance with Recommendation 1.

**Management response to Recommendation 2.** Concur. DON policy will require removal of hard drives and other external storage media prior to them being removed from DON control. The policy will ensure safeguards are in place to secure hard drives and external storage media prior to disposal or redistribution within DON.

DON policy will be developed within 90 days of the date of this memorandum. However, DON CIO will submit an update no later than 20 June 2009.

**Naval Audit Service comment on response to Recommendation 2.** Actions planned meet the intent of the recommendation. Though DON CIO states that they will develop the necessary policy in 90 days, in Recommendation 4, they state that they plan to have the recommendations implemented within 6 months of their management response letter. The interim target date will be 20 June 2009, and the final target completion date will be 30 October 2009.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**Recommendation 3.** Develop policy that requires the tracking (by serial or other identifying number) of all hard drives (classified and unclassified) once separated from a computer.

**Management response to Recommendation 3.** Concur. DON policy will include tracking guidance by serial or other identifier for all hard drives prior to disposal or redistribution.

DON policy will be developed within 90 days of the date of this memorandum. However, DON CIO will submit an update no later than 20 June 2009.

**Naval Audit Service comment on response to Recommendation 3.** Actions planned meet the intent of the recommendation. Though DON CIO states that they will develop the necessary policy in 90 days, in Recommendation 4 they state that they plan to have the recommendations implemented within 6 months of their management response letter. The interim target date will be 20 June 2009, and the final target completion date will be 30 October 2009.

The Commandant of the Marine Corps provided comments on Recommendation 3, which was addressed to DON-CIO. The Commandant suggested that there be a “modification to the recommendation to include the development of a common tool for use across the Department for tracking and reporting hard drives.” We appreciate the Commandant’s comment and agree that developing a common tool could be beneficial. We encourage the Marine Corps to address this issue with DON CIO as the new DON policy is developed.

**Recommendation 4.** Establish a plan of action and milestones for rapidly implementing Recommendations 1 through 3.

**Management response to Recommendation 4.** Concur. DON CIO will establish a plan of action and milestones for implementing guidance within 30 days of the release of DON policy. Implementation of all recommendations should be completed within 6 months from the date of this memorandum. However, DON CIO will submit an update no later than 20 June 2009.

**Naval Audit Service comment on response to Recommendation 4.** Actions planned meet the intent of the recommendation. DON CIO states that they plan to develop the necessary policy in 90 days, and they plan to have the recommendations implemented within 6 months of their

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

management response letter. The interim target date will be 20 June 2009, and the final target completion date will be 30 October 2009.

We recommend that Naval Network Warfare Command:

**Recommendation 5.** Develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). Coordinate with DON CIO to ensure NETWARCOM is prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Assign accountability for the actions required by this recommendation to specific office(s) or position(s).

**Management response to Recommendation 5.** Concur. Pending issuance of new DON CIO policy, NETWARCOM released Navy Telecommunications Directive (NTD) 12/08, "Disposition of Navy Computer Hard Drives." Within this interim directive, there are now only two approved disposition methods for all Navy Classified and CUI hard drives; either ship to National Security Agency (NSA) for disposition or use a NSA-certified disposal method (i.e. Commercial vendor or Navy organization equipped with NSA approved degaussers). Specific procedures for preparation and shipment of hard drives were provided in the NTD.

Exception to above policy: Due to contract obligations within the Navy and Marine Corps Intranet (NMCI), unclassified NMCI hard drives that reside outside the Navy Nuclear Propulsion Information (NNPI) and Navy Criminal Investigative Service (NCIS) Communities Of Interest (COI) are to be returned to the NMCI vendor (EDS). Unclassified NMCI hard drives used within the NNPI and NCIS COI must follow policy as outlined in NTP 12/08.

(Action): Establish Standard Operating Procedures (SOP) for the physical destruction of all Navy computer hard drives not sent to NSA for disposition. Procedures will be based on DON CIO policy and must provide 100 percent assurance that physically destroyed DON hard drives cannot be later made operational or their data accessible. Update NTD 12/08 to reflect DON CIO policy. Estimated Completion Date: 45 days after release of DON CIO policy.

**Naval Audit Service comment on response to Recommendation 5.**

Actions meet the intent of the recommendation. Because DON CIO plans to implement their new policy by 30 October 2009, the target completion date for this recommendation is 18 December 2009. While this is more than six months away, NETWARCOM must wait until the policy is established before they can take action.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**Recommendation 6.** Develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process.

**Management response to Recommendation 6.** Concur. NTD 12/08 directs internal controls via a signed destruction receipt from NSA (i.e. Classified material Conversion receipt for destruction). Commands using commercial vendors or Navy organizations must also provide a receipt for destruction similar to that of NSA. In either case, commands shall compare the signed notice of destruction with local accountability records (i.e. logbook or database).

(Action): Provide specific internal control measures for Command Security Managers and Information Assurance Managers on the proper separation and handling of classified and Controlled Unclassified Information (CUI) hard drives during the disposal process. Develop Navy standard form (for local command use) that tracks computer hard drives from separation to destruction. Estimated Completion Date: 60 days after release of DON CIO policy.

**Naval Audit Service comment on response to Recommendation 6.**

Actions meet the intent of the recommendation. Because DON CIO plans to implement their new policy by 30 October 2009, the target completion date for this recommendation is 30 December 2009. While this is more than six months away, NETWARCOM must wait until the policy is established before they can take action.

**Recommendation 7.** Develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.

**Management response to Recommendation 7.** Concur. Destruction records must associate the hard drive with a specific computer/component (Serial number, type, model and classification of hard drive is required). Commands are subject to oversight inspections by appropriate authorities to ensure compliance (i.e. Navy Audit Service, DISA Enhanced Compliance Validation (ECV), etc.). Command Security Managers and Information Assurance Managers have specific accountability, preparation, and administrative responsibilities for this process.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

(Action): Coordinate with DISA Enhanced Compliance Validation (ECV), Navy IG, Naval Audit Service, and CNO N09N2 (Information Security Program Authority) to include as part of inspection checklists during command visits. Work with appropriate authorities to include DON CIO policy as part of the Command Security Manager and Information Assurance Manager (IAM) training pipeline. Estimated Completion Date: 90 Days after release of DON CIO policy.

**Naval Audit Service comment on response to Recommendation 7.**

Actions meet the intent of the recommendation. Because DON CIO plans to implement their new policy by 30 October 2009, the target completion date for this recommendation is 29 January 2010. While this is more than six months away, NETWARCOM must wait until the policy is established before they can take action.

**Recommendation 8.** Establish a plan of actions and milestones for rapidly implementing Recommendations 5 through 7.

**Management response to Recommendation 8.** Concur. NETWARCOM will continue to work closely with DON CIO in the development of DON level policy and to facilitate timely execution of this policy throughout the enterprise once issued. Recommendations 5 through 7 to establish a POA&M meet this recommendation.

**Naval Audit Service comment on response to Recommendation 8.**

Actions meet the intent of the recommendation. Because Recommendations 5 through 7 directly affect Recommendation 8, the target completion date will be 29 January 2010. While this is more than six months away, NETWARCOM must wait until the policy is established before they can take action.

We recommend that the Commandant of the Marine Corps (CMC):

**Recommendation 9.**<sup>15</sup> Direct the appropriate HQMC organizations to develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). The

---

<sup>15</sup> The recommendation originally read "Direct the Marine Corps Network Operations and Security Center (MCNOSC) to develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). MCNOSC should coordinate with DON CIO to ensure MCNOSC is prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Direct MCNOSC to assign accountability for the actions required by this recommendation to specific office(s) or position(s)." This change was made based on comments from CMC stating that MCNOSC was not the appropriate level to develop and promulgate policy.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (AUDIT REPORT N2009-0027)**

appropriate organizations should coordinate with DON CIO to ensure they are prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Direct the appropriate HQMC organization to assign accountability for the actions required by this recommendation to specific office(s) or position(s).

**Management response to Recommendation 9.** Concur. Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI) HQMC C4 will work with HQMC Plans, Policies, and Operations (PP&O) and MCNOSC to develop and implement policies in executing the DON CIO policies. HQMC C4, PP&O, and MCNOSC will coordinate with DON CIO to ensure we are prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. HQMC C4, PP&O, and MCNOSC will assign accountability for the actions required by this recommendation to specific office(s) or position(s). A MCNOSC OpAdvisory will be issued. Estimated completion date is 30 days after issuance of the new DON CIO policy.

**Naval Audit Service comment on the response to Recommendation 9.** Actions planned meet the intent of the recommendation. DON CIO plans to implement their new policy by 30 October 2009, which places the target completion date for this recommendation at 30 November 2009. While this is more than six months away, Marine Corps must wait until the policy is established before they can take action.

**Recommendation 10.**<sup>16</sup> Direct the appropriate HQMC organization to develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process.

**Management response to Recommendation 10.** Concur. Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI) HQMC C4 will work with PP&O and MCNOSC to develop and implement internal controls at the regional level and provide separation and handling of classified, unclassified, and controlled unclassified information

---

<sup>16</sup> The recommendation originally read "Direct MCNOSC to develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process." This change was made based on comments from CMC stating that MCNOSC was not the appropriate level to develop and promulgate policy.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

hard drives during the disposal process. Estimated completion is 60 days after the issuance of the new DON CIO policy.

**Naval Audit Service comment on the response to Recommendation 10.** Actions planned meet the intent of the recommendation. DON CIO plans to implement their new policy by 30 October 2009, which places the target completion date for this recommendation at 30 December 2009. While this is more than six months away, Marine Corps must wait until the policy is established before they can take action.

**Recommendation 11.**<sup>17</sup> Direct the appropriate HQMC organization to develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.

**Management response to Recommendation 11.** Concur. Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI) HQMC C4 will work with PP&O and MCNOSC to develop and implement internal controls at the regional level and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives. Estimated completion is 60 days after the issuance of the new DON CIO policy.

**Naval Audit Service comment on the response to Recommendation 11.** Actions planned meet the intent of the recommendation. DON CIO plans to implement their new policy by 30 October 2009, which places the target completion date for this recommendation at 30 December 2009. While this is more than six months away, Marine Corps must wait until the policy is established before they can take action.

**Recommendation 12.** Establish a plan of action and milestones for rapidly implementing Recommendations 9 through 11.

**Management response to Recommendation 12.** Concur. POA&M will be developed upon receipt of recommended DON CIO policies.

---

<sup>17</sup> The recommendation originally read "Direct MCNOSC to develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives." This change was made based on comments from CMC stating that MCNOSC was not the appropriate level to develop and promulgate policy.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**Naval Audit Service comment on the response to Recommendation 12.**

Actions planned meet the intent of the recommendation. DON CIO plans to implement their new policy by 30 October 2009. In the cover letter to their response, Marine Corps gave us a target completion date of 60 days for this recommendation, which places the actual target completion date at 30 December 2009. While this is more than six months away, Marine Corps must wait until the policy is established before they can take action.

In his response to the recommendations, the Commandant of the Marine Corps noted that MCNOSC was not the appropriate level to be making policy. He stated that “USMC policy is developed and promulgated by HQMC and not by MCNOSC. Lead USMC organization responsible for CMS related matters is HQMC Plans, Policies, and Operations (PP&O). Recommend eliminate and replace MCNOSC and with “appropriate HQMC organization(s).” We agree with this change, and have revised the applicable recommendations.

We recommend that Program Executive Office – Enterprise Information Systems (PEO-EIS):

**Recommendation 13.**<sup>18</sup> Concurrent with DON CIO’s, NETWARCOM’s, and the Marine Corps’ efforts to address Recommendations 1 through 12, determine whether or not actions taken and planned require modifications to the existing NMCI contract. If so, identify the specific contract modifications that will need to be made, and initiate prompt action(s) to implement the modifications.

**Management response to Recommendation 13.** Concur. PMW-200 will determine the contract modifications necessary to implement the approved policy changes related to Recommendations 1 through 12. Actions necessary to implement the changes will be taken, and the Procuring Contract Officer will negotiate any required changes and costs with EDS.

**Naval Audit Service comment on the response to Recommendation 13.**

Actions planned meet the intent of the recommendation. In subsequent communications with PEO-EIS, they stated that PM NMCI will negotiate the necessary contract modifications within 90 days of receiving the required annual funding. The implementing procedural changes can then be implemented with EDS within 90 days of the contract modification. Because we cannot determine when annual funding will be acquired, or

---

<sup>18</sup> Recommendation 13 originally read: “Concurrent with DON CIO’s, NETWARCOM’s, and MCNOSC’s efforts to address Recommendations 1 through 12, determine whether or not actions taken and planned require modifications to the existing NMCI contract. If so, identify the specific contract modifications that will need to be made, and initiate prompt action(s) to implement the modifications.” This change was made based on comments from CMC stating that MCNOSC was not the appropriate level to develop and promulgate policy.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

when the contract modifications will be complete, PEO-EIS should give us an update on progress by 30 December 2009 (60 days after the completion of the DON CIO policy).

**Recommendation 14.** Ensure that policy, and procedure changes resulting from Recommendations 1 through 12 are made an integral part of the Next Generation Enterprise Network (NGEN) contract and related internal controls and governance processes.

**Management response to Recommendation 14.** Concur. PEO-EIS will work with ACNO NGEN System Program Office to integrate the changes into the contract and related internal controls and governance processes based on approved policy changes resulting from Recommendations 1 through 12.

**Naval Audit Service comment on the response to Recommendation 14.** Actions planned meet the intent of the recommendation. In subsequent communications with PEO-EIS, they stated that PM NMCI will negotiate the necessary contract modifications within 90 days of receiving the required annual funding. The implementing procedural changes can then be implemented with EDS within 90 days of the contract modification. Because we cannot determine when annual funding will be acquired, or when the contract modifications will be complete, PEO-EIS should give us an update on progress by 30 December 2009 (60 days after the completion of the DON CIO policy).

We recommend that the Assistant Secretary of the Navy (Research, Development and Acquisition):

**Recommendation 15.** Develop and implement an oversight plan that ensures that PEO-EIS has the necessary support and funding to implement Recommendations 13 and 14.

**Management response to Recommendation 15.** Concur. A plan will be developed based on the actions taken by the DON CIO, Naval Network Warfare Command and CMC to implement Recommendations 1-12 of the report. We will work directly with the appropriate resource sponsors to ensure that adequate funding is identified to implement the required solution.

A plan will be issued within 90 days of the publication of the final audit report.

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

**Naval Audit Service comment on response to Recommendation 15.**  
Actions planned meet the intent of the recommendation. The target completion date will be 31 July 2009.

## **6. Computers Approved for Release to the Public**

a. We found accessible DON sensitive data, including at least 605 unique SSNs, on 1 of the 112 computers EDS had cleared<sup>19</sup> and prepared for release to the public at the Mechanicsburg warehouse. According to the DON contract, all DON data should have been removed from the computer. Our test was conducted on 11 February 2008, and was a statistical sample of 112 computers from a universe of 4,174 scrubbed computers at the NMCI warehouse in Mechanicsburg, PA, that were ready for release to the public. EDS had performed the clearing procedure on the hard drives for all of these computers.<sup>20</sup> Thus, all DON data should have been removed and no longer be accessible on the hard drives. However, by using commercially available data recovery software, we were able to access DON sensitive data, including at least 605 unique SSNs, on 1 of the 112 EDS-cleared computers.<sup>21</sup> This occurred because the EDS scrubbing process in place at that time was not sufficient to ensure hard drives were properly cleared of data. At the time, EDS estimated that they would clear about 120,000 computers of DON data in calendar year 2008 and dispose of those computers. Therefore, the potential existed for 1,068<sup>22</sup> computers still containing sensitive DON data to be made available to the public if the scrubbing process was not corrected. We notified the PEO-EIS of this situation via a Draft Auditor General Alert issued on 25 February 2008 (see Enclosure 4).<sup>23</sup> In that Alert, we made four suggestions for prompt action. In immediate response to these suggestions, the PEO-EIS took actions to: immediately impose a DON-wide moratorium on EDS's release to the public of computers containing hard drives; begin analysis to determine what caused EDS to conclude that DON data had been cleared from the hard drive identified during testing; and initiate corrective actions to prevent similar occurrences in the future.

b. The PEO-EIS lifted the moratorium as a result of actions taken by EDS to implement improvements to the hard drive sanitization process, including: upgrading to the most current version of software; implementing a server-based configuration to eliminate as much as 95 percent of the personnel interaction to the process; implementing

---

<sup>19</sup> The auditors notified EDS's site management upon finding DON sensitive data on the hard drive, and EDS reportedly secured the hard drive.

<sup>20</sup> The DON contract with EDS requires EDS to "clear" information technology resources of all DON data. Those involved in the process usually refer to this as "scrubbing."

<sup>21</sup> The auditors notified EDS site management upon finding DON sensitive data on the hard drive, and EDS reportedly secured the hard drive.

<sup>22</sup> Our projection is based on EDS's estimate that they will refresh about 10,000 computers per month during calendar year 2008. We are 99 percent confident that our projection is accurate.

<sup>23</sup> The Draft Auditor General Alert notified the PEO-EIS that computers were being sold to the public that still contained DON and personal data after having gone through the scrubbing and verification process.

**FOR OFFICIAL USE ONLY**

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (AUDIT REPORT N2009-0027)**

an automated “active data recovery” tool scan on every drive following data destruction; and, establishing an automated logging console to record the actions taken and end-state disposition of every device.

c. The audit team assessed the impact of improvements put in place by the PEO-EIS and EDS in response to our 25 February 2008 draft Auditor General Alert. To do this; we tested a sample of 433 computers from a universe of 3,120<sup>24</sup> that were shipped from the Mechanicsburg warehouse used by EDS to a subcontractor facility in Georgia to be processed for sale to the public. Our objective was to determine if EDS’s corrective actions were effective. We found that all 433 computers<sup>25</sup> had been properly sanitized of data during the scrubbing process. It should be noted, however, that these results, while positive, were achieved by EDS after our audit findings brought high-level (ASN (RDA), the DON CIO, NETWARCOM, the PEO-EIS, and the Director NMCI) attention to EDS’ improper sanitizing of hard drives.

d. We are not making specific recommendations regarding the scrubbing process because of our overall recommendation that all hard drives be physically destroyed (see page 8, Recommendation 1).

**7. Other Information.**

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

b. Actions planned by the commands meet the intent of the Recommendations. These recommendations are considered open pending completion of the planned corrective actions, and are subject to monitoring in accordance with reference (b). Management should provide a written status report on the recommendations within 30 days after target completion dates. Please provide all correspondence to the Assistant Auditor General for Manpower and Reserve Affairs Audits, [REDACTED] by e-mail [REDACTED] with a copy to the Director, Policy and Oversight, [REDACTED] by e-mail at [REDACTED]. 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)

<sup>24</sup> Since the 3,120 computers were the first to be shipped after the moratorium was lifted, we do not consider the fact that all were found to be properly cleared of DON data to necessarily be indicative of future performance.

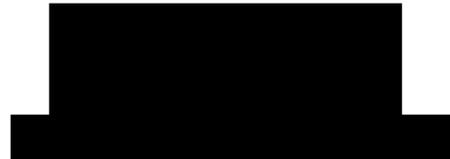
<sup>25</sup> The 433 computer sample consisted of 361 desktops and 72 laptops.

**~~FOR OFFICIAL USE ONLY~~**

Subj: **PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

c. 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).

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



FOIA  
(b)(6)

Assistant Auditor General  
Manpower and Reserve Affairs Audits

Distribution:

Assistant Secretary of the Navy (Research, Development, and Acquisition)  
Department of the Navy Chief Information Officer  
Commandant of the Marine Corps  
Commander, Naval Network Warfare Command  
Program Executive Officer (Enterprise Information Systems)

Copy to [next page]

**Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(AUDIT REPORT N2009-0027)**

Copy to:

UNSECNAV

OGC

ASSTSECNAV FMC

ASSTSECNAV FMC (FMO)

ASSTSECNAV IE

ASSTSECNAV MRA

CNO (VCNO, DNS-33, N4B, N41)

CMC (ACMC)

NAVINGEN (NAVIG-4)

CNR

BUMED

CHNAVPERS

COMNAVVAIRSYSCOM

COMNAVSEASYSYSCOM

COMNAVSUPSYSCOM

COMSPAWARSYSCOM

COMNAVFACENCOM

COMUSFLTFORCOM

COMPACFLT

CNIC

NETC

## Enclosure 1:

# Status of Recommendations

Recommendations							
Finding <sup>26</sup>	Rec. No.	Page No.	Subject	Status <sup>27</sup>	Action Command	Target or Actual Completion Date	Interim Target Completion Date
1	1	8	Develop policy that requires the timely and permanent <i>physical</i> destruction of <i>all</i> DON classified and unclassified hard drives (NMCI and non-NMCI) prior to the drives being removed from DON control (except for those being sent to the National Security Agency (NSA) for destruction in accordance with NETWARCOM Telecommunication Directive of 12/08). For hard drives not sent to NSA for destruction, the method(s) of destruction must physically destroy the hard drive (i.e., shredding or crushing the hard drive itself vs. only degaussing to destroy the data) and all data on it. The destruction method(s) identified in the DON CIO policy must provide 100 percent assurance that physically destroyed DON hard drives cannot later be made operational, and/or their data accessible.	O	DON CIO	10/30/09	6/20/09
1	2	10	Develop policy that requires all user organizations to ensure the removal of hard drives (classified and unclassified) from computers that will no longer be subject to DON control, and to ensure the hard drives are properly secured until they can be physically destroyed in accordance with Recommendation 1.	O	DON CIO	10/30/09	6/20/09
1	3	11	Develop policy that requires the tracking (by serial or other identifying number) of all hard drives (classified and unclassified) once separated from a computer.	O	DON CIO	10/30/09	6/20/09
1	4	11	Establish a plan of action and milestones for rapidly implementing Recommendations 1 through 3.	O	DON CIO	10/30/09	6/20/09

<sup>26</sup> / + = Indicates repeat finding.

<sup>27</sup> / 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.

Recommendations							
Finding <sup>26</sup>	Rec. No.	Page No.	Subject	Status <sup>27</sup>	Action Command	Target or Actual Completion Date	Interim Target Completion Date
1	5	12	Develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). Coordinate with DON CIO to ensure NETWARCOM is prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Assign accountability for the actions required by this recommendation to specific office(s) or position(s).	O	NETWARCOM	12/18/09	
1	6	13	Develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process.	O	NETWARCOM	12/30/09	
1	7	13	Develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.	O	NETWARCOM	1/29/10	
1	8	14	Establish a plan of actions and milestones for rapidly implementing Recommendations 5 through 7.	O	NETWARCOM	1/29/10	
1	9	14	Direct the appropriate HQMC organizations to develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). The appropriate organizations should coordinate with DON CIO to ensure they are prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Direct the appropriate HQMC organization to assign accountability for the actions required by this recommendation to specific office(s) or position(s).	O	CMC	11/30/09	

Recommendations							
Finding <sup>26</sup>	Rec. No.	Page No.	Subject	Status <sup>27</sup>	Action Command	Target or Actual Completion Date	Interim Target Completion Date
1	10	15	Direct the appropriate HQMC organization to develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process.	O	CMC	12/30/09	
1	11	16	Direct the appropriate HQMC organization to develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.	O	CMC	12/30/09	
1	12	16	Establish a plan of action and milestones for rapidly implementing Recommendations 9 through 11.	O	CMC	12/30/09	
1	13	17	Concurrent with DON CIO's, NETWARCOM's, and the Marine Corps' efforts to address Recommendations 1 through 12, determine whether or not actions taken and planned require modifications to the existing NMCI contract. If so, identify the specific contract modifications that will need to be made, and initiate prompt action(s) to implement the modifications.	O	PEO (EIS)	12/30/09	
1	14	18	Ensure that policy, and procedure changes resulting from Recommendations 1 through 12 are made an integral part of the Next Generation Enterprise Network (NGEN) contract and related internal controls and governance processes.	O	PEO (EIS)	12/30/09	
1	15	18	Develop and implement an oversight plan that ensures that PEO-EIS has the necessary support and funding to implement Recommendations 13 and 14.	O	ASN (RDA)	7/31/09	

## Enclosure 2:

# Scope and Methodology

---

## Scope

We conducted the audit during the period of 16 November 2007 through 6 March 2009. Our audit work focused on the disposal process for NMCI computers and hard drives. The disposition of Navy Marine Corps Intranet (NMCI) computers and unclassified hard drives is handled by Electronic Data Systems (EDS). A list of the activities we visited or contacted is included in this enclosure.

## Methodology

We interviewed the NMCI Program Management (PM) Office, EDS, and subcontract management officials to document the disposal process and obtained pertinent background information at selected Navy activities, Mechanicsburg, PA; San Diego, CA; and Ford Island, HI.

We briefed the NMCI PM Office, the Naval Criminal Investigative Service (NCIS), the U.S. Marine Corps Inspector General (USMC IG), Acquisition Integrity Office, and Department of the Navy Chief Information Officer (DON CIO) officials on preliminary audit results throughout the audit.

We reviewed contract and procedural guidance, policy, laws, and regulations applicable to the disposal of NMCI computers for clearing DON and personal data residing on the hard drives. This included the NMCI contract and attachments, Assistant Secretary of Defense Memorandum, Department of the Navy Guidance, Department of Defense Manuals, EDS procedural guidance, and other guidance (see Enclosure 3, Pertinent Guidance, for a listing and additional information).

We performed testing procedures to identify significant DON risks (see details below) involving the disposition of unclassified and classified computers and hard drives that still contained sensitive information. Specifically, we:

- Tested EDS scrubbing procedures at Mechanicsburg, PA;
- Performed follow-up testing at the subcontractor facility using forensic software;

- Met with NCIS to determine the best testing method, use of forensic software, and subject matter experts;
- Utilized statisticians from the Defense Contract Audit Agency (DCAA) and Naval Audit Service who recommended statistical sampling techniques such as discovery sampling for testing hard drives. We made statistical projections of documents with Social Security numbers (SSNs) based on our sample of 60 hard drives;
- Tested classified and unclassified hard drives using commercially available forensic software to determine whether DON data existed on them;
- Performed a physical count of 2,050 hard drives at Ford Island, HI and a physical inventory of the 2,449 hard drives at Mechanicsburg, PA;
- Matched degaussing documentation found at Ford Island, HI against serial numbers of hard drives to identify classified hard drives with no markings for further testing;
- Performed analytical tests on selected classified and unclassified hard drives to determine that personally identifiable information (PII) and DON official data existed on them; and
- Received NCIS and Navy Supply Information Systems Activity (NSISA) assistance and training on the use of forensic software; specifically Forensic Toolkit (FTK), Computer Forensic and Data Recovery Software (WINHEX), and EnCase Forensic Software.

We stored classified hard drives in an NCIS facility, and for those no longer needed, sent selected hard drives to the National Security Agency (NSA) for destruction.

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

During the audit, we contacted or visited the following activities:

- NMCI Program Office, Crystal City, VA
- NMCI/EDS Warehouse, Naval Support Activity, Mechanicsburg, PA
- NMCI/EDS Warehouse, San Diego, CA
- NMCI/EDS Warehouse, Ford Island, HI

- NMCI Storage Facility, Washington Navy Yard, Washington, DC
- NMCI Cross Dock Warehouse, Andrews Air Force Base, MD
- Assistant for Administration to the Under Secretary of the Navy (AAUSN)
- Navy Supply Information Systems Activity (NSISA), Mechanicsburg, PA
- Apto Solutions, Atlanta, GA
- Global Investment Recovery, Salley, SC
- NCIS field office and testing facility, Washington Navy Yard, DC
- USMC IG, Arlington, VA
- DCAA, Fort Belvoir, VA
- White Canyon Technical Support Staff, Orem, UT
- National Security Agency, Fort Meade, MD

We evaluated internal controls and reviewed compliance with regulations. There were no prior audits done within the past 5 years regarding the NMCI computer disposal process. Therefore, the normal followup process was not required.

## Federal Managers' Financial Integrity Act (FMFIA)

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 1-3 address issues related to the internal control over classified computer hard drives. In our opinion, the weaknesses noted in this report may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

## Communication with Management

The audit team maintained a close relationship with the staff of the NMCI Program Management Office. Meetings were scheduled every 2 to 3 weeks to update audit progress and provide timely information. Audit staff corresponded often with the NMCI Program Manager by providing information or submitting requests for information. The Assistant Auditor General updated the Program Executive Office for Enterprise Information Systems (PEO-EIS) on key issues as they evolved.

## Enclosure 3:

# Pertinent Guidance

---

- **Assistant Secretary of Defense Memorandum, Disposition of Unclassified DoD Computer Hard Drives, dated June 4, 2001:**

This guidance is applicable to all Department of Defense (DoD)-owned or controlled hard drives and therefore applicable to the contractor, EDS, and their overwrite procedures.

Attachment 1, Section 2.1. states:

The individual performing the overwriting must be properly trained and will be responsible for certifying that the process has been successfully completed.

“If the hard drive is determined to be not repairable and is to be removed from service, the contractor may degauss or destroy the hard drive, or return the drive to DOD for degaussing or destruction, depending on the terms of the lease agreement. If the contractor is responsible for the destruction or degaussing of the drives, the contractor will certify in writing that this process has been completed in accordance with one of the methods specified in Attachment 2.”

- **DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006:**

Classified material removed from a cleared facility for destruction shall be destroyed on the same day it is removed.

- **Navy Marine Corps Intranet (NMCI) Conformed Contract, Section 6.10 - Security Requirements, awarded October 6, 2000:**

The Contractor shall comply with the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DOD 5220.22-M), and any revisions to that manual.

- **IA Pub-5239-26, Department of the Navy (DON) Information Assurance Remanence Security Publication, May 2000:**

Degaussing with approved degaussing equipment is a method for purging operational and non-operational magnetic data storage media, and is an alternative to physical destruction of magnetic data storage media.

- **Secretary of the Navy (SECNAV) M-5510.36, DON Information Security Program (ISP), dated 30 June 2006:**

This policy manual applies to all personnel, military and civilian, assigned to or employed by any element of DON, and includes cleared contractor visitors working under the purview of a commanding officer. The manual establishes the minimum standards for classifying, safeguarding, transmitting and destroying classified information as required by higher authority.

**Removable Storage Media Markings.** Mark classified removable IT storage media with the highest overall classification level using the appropriate label. Removable IT storage media is any device in which classified data is stored and is removable from a system by the user or operator (i.e., optical disks, magnetic diskettes, removable hard drives, thumb drives, tape cassettes, etc.).

Each IT system shall be marked to indicate the highest classification level of the information processed by the IT system and the network to which it is connected. The appropriate label shall be placed on IT systems and components with memory such as workstations, external hard drives, printers, copiers, portable electronic devices, servers, and back-up devices.

Classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container, vault, modular vault, or secure room.

- **NMCI Information Advisory 06-03, Classified Hard Drive Disposition Procedures:**

This information advisory shall be used for disposition of classified hard drives from the legacy and NMCI networks during both transition and steady state operations.

**A. Assumption of responsibility (AOR) to cutover.** Upon Information Strike Force (ISF) AOR, of the legacy network and throughout transition to NMCI, the government will maintain control and accountability of all legacy classified hard drives in accordance with applicable security policies and procedures. Disposition of legacy hard drives at cutover remains the responsibility of the government, method of disposition (i.e., purging or destruction) is left to the discretion of the transitioning command.

Hard drives that are destined for destruction should be retained by the Government, withheld from the inventory provided to the ISF at the time of AOR, and shall be annotated on the site concurrence memorandum.

**B. Post-Cutover.** In the context of NMCI, all classified hard drives residing on the network are owned by ISF and should therefore be returned to the contractor's possession upon replacement (e.g., tech-refresh or unrecoverable failure), in accordance with guidance set forth in Commander Naval Network Warfare Command Instruction (COMNAVNETWARCOMINST) 5239.1; all classified hard drives must be degaussed before transferring to ISF control. Because proper degaussing effectively declassifies hard drives, subsequent physical destruction is not required. Hard drives subsequently transferred to ISF under these procedures become the responsibility of ISF.

- **Navy Telecommunications Directive (NTD)12/08, Disposition of Navy Computer Hard Drives, December 2008:**

This interim policy applies to all Navy commands using classified (collateral only) and unclassified hard drives connected to Navy networks to include, but not limited to NMCI, ONE-NET, IT21, legacy and excepted networks. This interim policy applies to both internal and removable hard drives. In the case of NMCI, all classified hard drives and all controlled unclassified information (CUI) hard drives within the Naval Nuclear Propulsion Information (NNPI) and Naval Criminal Investigative Service (NCIS) communities of interest (COI) shall not be turned over to Electronic Data Systems (EDS) during tech refresh. All disposition responsibilities for such hard drives shall remain within the Government and carried out in accordance with this directive.

There are two approved disposition methods for Navy computer hard drives:

(1) Ship to the National Security Agency (NSA) for degaussing and crushing. And shall be reviewed by the command information assurance manager (IAM) and command security manager (CSM) for implementation and coordination.

(2) Use a service which is certified by NSA as an NSA-approved disposal method. There are commercial vendors who do this on site as well as Navy organizations such as Space and Naval Warfare Systems Command (SPAWAR) which have a National Security Agency (NSA)-approved capability. A command may use either method, but will bear whatever cost is associated with either the packaging and shipping of hard drives to NSA or with using the second method. Additionally, if a command is using a method other than NSA, they are responsible for documenting in their accountability record the validity of the destruction organizations NSA certification.

**Accountability and control.** Upon immediate removal from the network, the command IAM, in conjunction with the CSM, will ensure accurate records are maintained for each hard drive (by serial number, type, model, and classification)

being disposed of. Local accountability records must associate the hard drive to a specific computer/component and can be accomplished using a database or logbook.

**Administrative recording of final disposition.** Components are not considered destroyed until signed notice of destruction (e.g., classified material conversion (CMC) receipt for destruction of classified material, or similar form) is received from the approved destruction organization. Once received, commands shall compare the signed notice of destruction with local accountability records (i.e. database or logbook) to ensure applicable media has been properly disposed of.

- **Navy Marine Corps Intranet Contract, Attachment 4 - Security Requirements, Section 1.1.4.3 - Privacy and Security Safeguards, awarded October 6, 2000:**

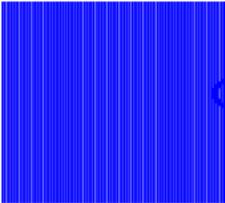
“The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) is cleared of all DON data and sensitive application software by a technique approved by the government. For IT resources leaving DON use, applications acquired with a "site license" or "server license" shall be removed. Damaged IT storage media will be degaussed and destroyed.”

- **Navy Marine Corps Intranet Asset Disposition Procedures Manual, Update Version 2.0., dated February 15, 2005:**

On page 3, Section 2, “Equipment Disposition Procedure,” EDS lists the steps, actions, roles, and responsibilities that comprise the equipment disposition procedure. Step 11 deals with inoperable hard drives and the responsibility for this step is assigned to the Scrub Team.

**Enclosure 4:**

# **Auditor General Alert of 25 February 2008**



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

7510  
N2008-NFO000-0025  
25 Feb 08

DRAFT AUDITOR GENERAL ALERT

MEMORANDUM FOR PROGRAM EXECUTIVE OFFICER FOR ENTERPRISE  
INFORMATION SYSTEMS (PEO/EIS))

Subj: **APPARENT RISK IN THE NAVY MARINE CORPS INTRANET  
(NMCI) COMPUTER TURN-IN AND DISPOSAL PROCESS  
(N2008-NFO000-0025)**

1. **Introduction.** This draft Auditor General Alert suggests that you take immediate action to mitigate what appears to be a significant risk of release of Department of the Navy (DON) data and Personally Identifying Information (PII). The risk was identified during the early stages of our ongoing audit of the Navy Marine Corps Intranet (NMCI) Computer Turn-In and Disposal Process. As our audit progresses and we complete additional work related to the subject issue, we are likely to make recommendations that include or are similar to the suggestions contained in this Alert. If we ultimately make recommendations, Secretary of the Navy Instruction 7510.F requires the recommendation addressee(s) to provide a formal written response that indicates actions taken and planned. This draft Alert does not require a formal response. However, given the time-sensitive nature of our findings, we would appreciate being advised in writing as soon as possible of corrective actions you plan to take in response to Suggestion 1. Our future report(s) will recognize actions taken in response to all suggestions contained in this Alert. A brief description of our preliminary findings and suggestions follows.

## 2. Preliminary Findings.

a. When NMCI computers are turned in to Electronic Data Systems Corporation (EDS) as the result of either the “tech refresh” process or for other reasons,<sup>28</sup> EDS, as the DON NMCI contractor, is responsible for clearing<sup>29</sup> the hard drives of all DON data, and then disposing of the computers. EDS disposes of computers primarily through sales to the public, donations, employee buybacks, and destruction. Based on EDS’s tech refresh estimate, they should clear about 120,000 computers of DON data in calendar year 2008 and dispose of those computers. Because NMCI computers are often used by DON employees for such things as storing, analyzing, and emailing sensitive data, it is likely that most of the computers that EDS has the responsibility to clear and dispose of, have had and will have sensitive DON data on them when they are turned in to EDS.

b. On 11 February 2008, we tested a random sample of 112 computers at the NMCI warehouse in Mechanicsburg, PA, that were ready for release to the public. EDS had performed the clearing procedure on the hard drives of all of these computers. Thus, all DON data should have been removed and no longer be accessible on the hard drives. However, by using commercially available data recovery software, we found accessible DON sensitive data on 1 of the 112 EDS-cleared computers.<sup>30</sup> Prior to our testing, this computer had also been subjected to a follow-on second check by EDS as part of its internal control program of rechecking 20 percent of already-cleared computers. Although we have not finished analyzing the accessible data we found on the hard drive, we know it contains PII (at least 605 unique Social Security Numbers identified to date) and what are likely pornographic images.<sup>31</sup> We have done a statistical projection to demonstrate the potential magnitude of the vulnerability that may exist as a result of EDS not successfully clearing all NMCI hard drives. Based on our statistical analysis, we project that, of the 120,000 computers EDS should clear in calendar year 2008, potentially 1,068<sup>32</sup> computers still containing sensitive DON data could be made available to the public if corrective action is not immediately taken. Some of the 1,068 computers may have already been released to the public in early 2008, and other computers containing DON sensitive data may have been released in prior years. Additional computers containing sensitive data could also be released in the future if current clearing procedures are not improved.

3. **Suggestions.** In order to ensure that no computers containing DON data are released to the public, we strongly suggest that you take the following actions.

---

<sup>28</sup> NMCI computers are also turned in to EDS because they are inoperative or excess.

<sup>29</sup> The DON contract with EDS requires EDS to “clear” information technology resources of all DON data. Those involved in the process usually refer to this as “scrubbing.”

<sup>30</sup> The auditors notified EDS site management upon finding DON sensitive data on the hard drive, and EDS reportedly secured the hard drive.

<sup>31</sup> We plan to refer this issue to the Naval Criminal Investigative Service and the Naval Inspector General.

<sup>32</sup> Our projection is based on EDS’s estimate that they will refresh about 10,000 computers per month during calendar year 2008. We are 99 percent confident that our projection is accurate.

**Suggestion 1.** Immediately impose a DON-wide moratorium on EDS's release to the public (including sales to the public, donations, and employee buybacks) of computers containing hard drives. The moratorium should stay in effect until Suggestion 4 is implemented. An alternative to disposing of the computers with hard drives intact would be to destroy the hard drives and dispose of the computers separately.

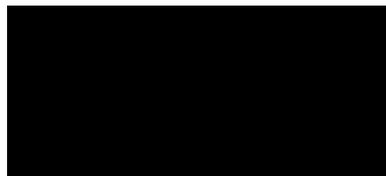
**Suggestion 2.** Determine what caused EDS to conclude all DON data had been cleared from the hard drive in question when it had not been.

**Suggestion 3.** Once the cause(s) in Suggestion 2 have been identified, take corrective actions that will prevent the same or similar occurrences.

**Suggestion 4.** Implement monitoring procedures to verify that corrective actions taken in response to Suggestion 3 are resulting in the clearing of all DON data from the hard drives of computers being made available for release to the public.

4. My staff and I will contact you to arrange a meeting where we can provide additional details regarding this issue and to discuss our progress and plans for the ongoing audit. I can be reached at [REDACTED] or at [REDACTED]. [REDACTED] the Audit Director responsible for this effort, and can be reached at [REDACTED] or at [REDACTED].

FOIA (b)(6)



Assistant Auditor General  
Manpower and Reserve Affairs Audits

Copy to:  
ASSTSECNAV MRA  
ASSTSECNAV RDA  
CNO (N1, N6, DNS-36)  
DON CIO  
NETWARCOM  
CMC (DCMC MRA)

**Enclosure 5:**

**Management Response from Department of the Navy  
Chief Information Officer and Assistant Secretary of the  
Navy (Research, Development, and Acquisition)**



DEPARTMENT OF THE NAVY  
CHIEF INFORMATION OFFICER  
1000 NAVY PENTAGON  
WASHINGTON, DC 20350-1000

~~FOR OFFICIAL USE ONLY~~

27 April 2009

This management response is not being marked "For Official Use Only" in this report.

MEMORANDUM FOR NAVAL AUDIT SERVICE

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (N2008-NFO0000-0025.001)

Ref: (a) NAVAUDSVC Draft Audit Report N2008-NFO000-0025.001 of 6 Mar 09

Encl: (1) ASN (RD&A) memo to DON CIO undated  
(2) NAVNETWARCOM comments of 7 Apr 09  
(3) PEO-EIS memo of 8 Apr 09  
(4) CMC (P&R (RFR)) memo of 13 Apr 09

After review of reference (a) and responses from Department of the Navy stakeholders, the Department of the Navy Chief Information Officer (DON CIO) concurs with the Naval Audit Service (NAVAUDSVC) recommendations. The DON CIO will take the necessary steps to develop policy that results in permanent destruction of all computer hard drives and external storage media that is either turned in as excess equipment or re-distributed to another end user. It should be noted that the Program Executive Officer for Enterprise Information Systems (PEO EIS) and Assistant Secretary of the Navy for Research and Development (ASN RD&A) have stated general concurrence but cited concern regarding the unfunded cost of implementing a hard drive physical destruction policy. While funding is a concern, ASN (RD&A) stated in enclosure (1) they will develop a plan that ensures PEO EIS has the necessary support and funding to destroy all classified and unclassified hard drives. The ASN (RD&A) also expressed concern about the contractual implications of this new policy.

Naval Network Warfare Command (NAVNETWARCOM) submitted comments to NAVAUDSVC responding to recommendations 5 through 8 in enclosure (2). PEO-EIS submitted comments to NAVAUDSVC responding to recommendations 13 and 14 in enclosure (3). Commandant of the Marine Corps (CMC) (P&R (RFR)) submitted comments to NAVAUDSVC responding to recommendations 9 through 12 in enclosure (4).

**Recommendation 1.** Develop policy that requires the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI) prior to the drives being removed from DON control except for those being sent to the National Security Agency (NSA) for destruction in accordance with NETWARCOM Telecommunication Directive of 12/08). For hard drives not sent to NSA for destruction, the method(s) of destruction must physically destroy the hard drive (i.e., shredding or crushing the hard drive itself vs. only degaussing to destroy the data) and all data on it. The destruction method(s) identified in the DON CIO policy, must provide 100 percent assurance that physically destroyed DON hard drives cannot later be made operational, and/or their data accessible.

— FOR OFFICIAL USE ONLY —

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE NAVY MARINE  
CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (N2008-NFO0000-  
0025.001)

**DON CIO Response:** Concur. The cost of physically destroying all hard drives (less those sent to NSA) is an unfunded requirement but the benefits to the DON outweigh those costs by ensuring no classified information or sensitive but unclassified information, including personally identifiable information (PII), is compromised. The cost of data spillages and PII breaches is incalculable, negatively impacts our personnel, stresses already constrained command resources and tarnishes our public image with the perception that our data is not properly safeguarded. The Department cannot continue with a policy that mitigates the risk but rather, it must implement and enforce a strict disposal/redistribution process with proper controls in place to ensure, with complete accuracy and timeliness, that all hard drives are physically destroyed. This risk avoidance policy will apply to all hard drives and all external media with memory, including servers, routers, switches, and external portable hard drives no longer under government control.

DON Policy will be developed within 90 days of the date of this memorandum.

**Recommendation 2.** Develop policy that requires all user organizations to ensure the removal of hard drives (classified and unclassified) from computers that will no longer be subject to DON control, and to ensure the hard drives are properly secured until they can be physically destroyed in accordance with Recommendation 1.

**DON CIO Response:** Concur. DON policy will require removal of hard drives and other external storage media when no longer under government control or when redistributed to another end user. The policy will ensure safeguards are in place to secure hard drives and external storage media prior to disposal or redistribution.

DON policy will be developed within 90 days of the date of this memorandum.

**Recommendation 3.** 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 CIO Response:** Concur. DON policy will include tracking guidance by serial or other identifier for all hard drives prior to disposal or redistribution.

DON policy will be developed within 90 days of the date of this memorandum.

**Recommendation 4.** Establish a plan of action and milestones for rapidly implementing Recommendations 1 through 3.

**DON CIO Response:** Concur.

— FOR OFFICIAL USE ONLY —

~~FOR OFFICIAL USE ONLY~~

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE NAVY MARINE  
CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS (N2008-NFO0000-  
0025.001)

DON will establish a plan of action and milestones for implementing guidance within 30 days of the release of DON policy. Implementation of all recommendations should be completed within six months from the date of this memorandum.

**Recommendation 15.** Develop and implement an oversight plan that ensures that PEO EIS has the necessary and funding to implement Recommendation 13 and 14.

**ASN RD&A Response:** Concur. A plan will be developed based on the actions taken by the DON CIO, Naval Network Warfare Command and CMC to implement Recommendations 1-12 of the report. We will work directly with the appropriate resource sponsors to ensure that adequate funding is identified to implement the required solution.

A plan will be issued within 90 days of publication of the final audit report.

This memorandum contains information that is deemed "For Official Use Only." We will submit our next update no later than 20 June 2009. Please address questions or comments to

[REDACTED]

[REDACTED]

FOIA (b)(6)

Copy to:  
ASN (RD&A)  
PEO EIS  
CNO (N6, N09B2)  
CMC (DMCS, C4)  
NAVNETWARCOM (N6)

~~FOR OFFICIAL USE ONLY~~

Enclosure 6:

# Management Response from Commandant of the Marine Corps



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
3030 MARINE CORPS PENTAGON  
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:  
7510  
HQMC C4 CP  
6 April 2009

From: Director, Command, Control, Communications, and Computers  
Department (C4)  
To: Headquarters Marine Corps, Programs and Resources,  
Audit and Review Branch (RFR)  
Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(NAVAUDSVC DRAFT AUDIT REPORT N2008-NFO000-0025.001)  
Ref: (a) NAVAUDSVC memo 7510/N2008-NFO000-0025.001, dated  
6 Mar 09  
(b) SECNAV Instruction 7510.7F, "Department of the Navy  
Internal Audit"

1. Reference (a) transmitted the subject draft report requesting Marine Corps comments. Draft report has been reviewed. HQMC C4 concurs with the audit report in that "strengthening policies and procedures over the disposal process, including, but not limited to, requiring the physical destruction of all hard drives being removed from DON control" would be helpful in mitigating national security and identify theft risks resulting from unauthorized access to classified and sensitive DON information.

The following are HQMC C4 comments on recommendations assigned to DON CIO:

- a. Recommendation 1. Concur. Recommend modification of recommendation to identify a specific time period for destruction of hard drive; as written, use of the word "timely" is subjective.
- b. Recommendation 2. Concur.
- c. Recommendation 3. Concur. Recommend modification of recommendation to include the development of a common tool for use across the Department for tracking and reporting hard drives.
- d. Recommendation 4. Concur.

Enclosure (7)

Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(NAVAUDSVC DRAFT AUDIT REPORT N2008-NFO000-0025.001)

Recommendation 13 assigned to PEO EIS should be revised to reflect comments made on recommendations 9 through 11 with respect to MCNOSC.

2. Per reference (b), the following comments are provided in response to the Naval Audit Service recommendations addressed to the Commandant of the Marine Corps (CMC):

a. Recommendation 9. CMC direct the Marine Corps Network Operations and Security Center (MCNOSC) to develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3 of draft report N2008-NFO000-0025.001). MCNOSC should coordinate with DON CIO to ensure MCNOSC is prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. CMC direct MCNOSC to assign accountability for the actions required by this recommendation to specific office(s) or position(s).

Marine Corps Response: Partially Concur. USMC policy is developed and promulgated by HQMC and not by MCNOSC. Lead USMC organization responsible for CMSS related matters is HQMC Plans, Policies, and Operations (PP&O). Recommend eliminate replace MCNOSC and with "appropriate HQMC organization(s)."

Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI), HQMC C4 will work with HQMC Plans, Policies, and Operations (PP&O) and MCNOSC to develop and implement policies in executing the new DON CIO policies. HQMC C4, PP&O, and MCNOSC will coordinate with DON CIO to ensure we are prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. HQMC C4, PP&O, and MCNOSC will assign accountability for the actions required by this recommendation to specific office(s) or position(s). A MCNOSC OpAdvisory will be issued. Estimated completion is 30 days after issuance of the new DON CIO policy.

b. Recommendation 10. CMC direct MCNOSC to develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process.

Marine Corps Response: Partially Concur. USMC policy is developed and promulgated by HQMC and not by MCNOSC. Lead USMC

Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(NAVAUDSVC DRAFT AUDIT REPORT N2008-NFO000-0025.001)

organization responsible for CMSS related matters is HQMC Plans, Policies, and Operations (PP&O). Recommend eliminate replace MCNOSC and with "appropriate HQMC organization(s)."

Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI), HQMC C4 will work with PP&O and MCNOSC to develop and implement internal controls at the regional level and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and controlled unclassified information hard drives during the disposal process. Estimated completion is 60 days after the issuance of the new DON CIO policy.

c. Recommendation 11. CMC direct MCNOSC to develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.

Marine Corps Response: Partially Concur. USMC policy is developed and promulgated by HQMC and not by MCNOSC. Lead USMC organization responsible for CMSS related matters is HQMC Plans, Policies, and Operations (PP&O). Recommend eliminate replace MCNOSC and with "appropriate HQMC organization(s)."

Upon development of the new DON CIO policy requiring the timely and permanent physical destruction of all DON classified and unclassified hard drives (NMCI and non-NMCI), HQMC C4 will work with PPO and MCNOSC to develop and implement internal controls at the regional level and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives. Estimated completion is 60 days after the issuance of the new DON CIO policy.

d. Recommendation 12. CMC establish a plan of action and milestones for rapidly implementing Recommendations 9 through 11.

Marine Corps Response: Concur. POA&M will be developed upon receipt recommended DON CIO policies.

3. The HQMC C4 point of contact is [REDACTED] who can be reached at [REDACTED] and email [REDACTED]

FOIA (b)(6)

Subj: PROCESSING OF COMPUTERS AND HARD DRIVES DURING THE NAVY  
MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL PROCESS  
(NAVAUDSVC DRAFT AUDIT REPORT N2008-NFO000-0025.001)

4. This report does contain information that is deemed "For Official Use Only".



Other than Personally Identifiable Information, no material in this report is being marked "For Official Use Only" or withheld from public release.

FOIA (b)(6)

Enclosure 7:

# Management Response from Commander, Naval Network Warfare Command



DEPARTMENT OF THE NAVY  
COMMANDER  
NAVAL NETWORK WARFARE COMMAND  
2405 GUADALCANAL RD  
NORFOLK, VA 23521-3228

IN REPLY REFER TO:

5000  
Ser N5/204  
22 Apr 09

From: Commander, Naval Network Warfare Command  
To: Mr. Jonathan Kleinwaks, Assistant Auditor General  
(Manpower and Reserve Affairs Audits) Naval Audit Service  
Subj: NAVAL AUDIT SERVICE RECOMMENDATIONS - DISPOSITION OF NAVY  
COMPUTER HARD DRIVES

1. Department of the Navy Chief Information Officer (DON CIO), Chief of Naval Operations (CNO) N09N2 (Information Security Program Authority) and Naval Network Warfare Command (NAVNETWARCOM) recognize Navy is not adhering to established procedures for the proper disposition and handling of classified and Controlled Unclassified Information (CUI) stored on electronic media. To mitigate further incidents - and while awaiting pending DON CIO policy as recommended by the Naval Audit Service (i.e., recommendations 1 through 3) - NAVNETWARCOM issued interim procedures via official naval message for disposition of Navy Classified and CUI hard drives once permanently removed from the network. These new procedures will be summarized individually as they apply to Naval Audit Service recommendations for NAVNETWARCOM (i.e., recommendations 5 through 8) below:

a. Recommendation 5: Develop and implement policies and procedures for user organizations and contractors to use in executing the new DON CIO policies (Recommendations 1, 2, and 3). Coordinate with DON CIO to ensure NAVNETWARCOM is prepared to issue implementing policies and procedures concurrent with DON CIO's release of new policies. Assign accountability for the actions required by this recommendation to specific office(s) or position(s).

(1) Response: Concur. Pending issuance of new DON CIO policy, NAVNETWARCOM released Navy Telecommunications Directive (NTD) 12/08, "Disposition of Navy Computer Hard Drives." Within this interim directive, there are now only two approved disposition methods for all Navy classified and CUI hard drives; either ship to National Security Agency (NSA) for disposition or use a NSA-certified disposal method (i.e., commercial vendor or Navy organization equipped with NSA approved degaussers).

Subj: NAVAL AUDIT SERVICE RECOMMENDATIONS - DISPOSITION OF NAVY  
COMPUTER HARD DRIVES

Specific procedures for preparation and shipment of hard drives were provided in the NTD.

(2) Exception to above policy: Due to contract obligations within the Navy Marine Corps Intranet (NMCI), unclassified NMCI hard drives that reside outside the Navy Nuclear Propulsion Information (NNPI) and Naval Criminal Investigative Service (NCIS) Communities of Interest (COI) are to be returned to the NMCI vendor (Electronic Data Systems). Unclassified NMCI hard drives used within the NNPI and NCIS COI must follow policy as outlined in NTD 12/08.

b. Recommendation 6: Develop and implement internal controls and provide oversight to ensure compliance with policies regarding the proper separation and handling of classified, unclassified, and CUI hard drives during the disposal process.

(1) Response: Concur. NTD 12/08 directs internal controls via a signed destruction receipt from NSA (i.e., Classified Material Conversion Receipt for Destruction). Commands using commercial vendors or Navy organizations must also provide a receipt for destruction similar to that of NSA. In either case, commands shall compare the signed notice of destruction with local accountability records (i.e., logbook or database).

c. Recommendation 7: Develop and implement internal controls and provide oversight to ensure immediate and continued compliance with DON CIO policies pertaining to the destruction of classified and unclassified hard drives.

(1) Response: Concur. Destruction records must associate the hard drive with a specific computer/component (Serial number, type, model, and classification of hard drive is required). Commands are subject to oversight inspections by appropriate authorities to ensure compliance (i.e., Naval Audit Service, Defense Information Systems Agency (DISA) Enhanced Compliance Validation (ECV), etc.). Command Security Managers and Information Assurance Managers have specific accountability, preparation, and administrative responsibilities for this process.

Subj: NAVAL AUDIT SERVICE RECOMMENDATIONS - DISPOSITION OF NAVY  
COMPUTER HARD DRIVES

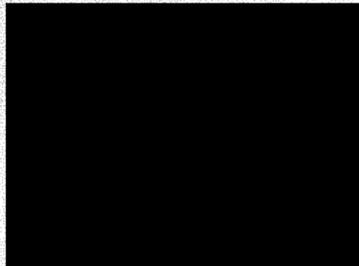
d. Recommendation 8: Establish a Plan of Actions and Milestones (POA&M) for rapidly implementing Recommendations 5 through 7.

(1) Response: Concur. NAVNETWARCOM will continue to work closely with DON CIO in the development of Department of the Navy level policy and to facilitate timely execution of this policy throughout the enterprise once issued. To that end, the following POA&M is established to meet recommendations 5 through 7 above:

(a) Recommendation 5 (action): Establish Standard Operating Procedures for the physical destruction of all Navy computer hard drives not sent to NSA for disposition. Procedures will be based on DON CIO policy and must provide 100 percent assurance that physically destroyed DON hard drives cannot be later made operational or their data accessible. Update NTD 12/08 to reflect DON CIO policy. Estimated Completion Date: 45 days after release of DON CIO policy.

(b) Recommendation 6 (action): Provide specific internal control measures for Command Security Managers and Information Assurance Managers on the proper separation and handling of classified and CUI hard drives during the disposal process. Develop Navy standard form (for local command use) that tracks computer hard drives from separation to destruction. Estimated Completion Date: 60 days after release of DON CIO policy.

(c) Recommendation 7 (action): Coordinate with DISA ECV, Navy Inspector General, Naval Audit Service, and CNO N09N2 (Information Security Program Authority) to include as part of inspection checklists during command visits. Work with appropriate authorities to include DON CIO policy as part of the Command Security Manager and Information Assurance Manager training pipeline. Estimated Completion Date: 90 days after release of DON CIO policy.



FOIA (b)(6)

Enclosure 8:

# Management Response from Program Executive Officer (Enterprise Information Systems)



DEPARTMENT OF THE NAVY  
PROGRAM EXECUTIVE OFFICER  
ENTERPRISE INFORMATION SYSTEMS (PEO-EIS)  
2451 CRYSTAL DRIVE, SUITE 1139  
ARLINGTON, VA 22202

7510  
Ser PEO-EIS/00063  
08 Apr 09

MEMORANDUM FOR NAVAL AUDIT SERVICE

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE  
NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL  
PROCESS (N2008-NFO000-0025.001)

Ref: (a) NAVAUSVC Draft Audit Report N2008-NFO000-0025.001  
dated 6 MAR 09

1. After review of reference (a), Program Executive Officer, Enterprise Information Systems (PEO (EIS)) concurs--with reservations--with the Naval Audit Service recommendations. The Program Manager for the Navy Marine Corps Intranet (PM, NMCI) will take the appropriate steps necessary to implement those recommendations as outline below.

Recommendation 1: Develop policy that requires the timely and permanent **physical** destruction of **all** DON classified and unclassified hard drives (NMCI and non-NMCI) prior to the drives being removed from DON control (except for those being sent to the National Security Agency (NSA) for destruction in accordance with NETWARCOM Telecommunication Directive of 12/08). For hard drives not sent to NSA for destruction, the method(s) of destruction must physically destroy the hard drive (i.e., shredding or crushing the hard drive itself vs. only degaussing to destroy the data) and all data on it. The destruction method(s) identified in the DON CIO policy, must provide 100 percent assurance that physically destroyed DON hard drives cannot later be made operational, and/or their data accessible.

PEO-EIS Comment: While Recommendation 1 would provide a more final solution to the potential loss of PII during the NMCI technical refresh process, PMW-200 is concerned with the unfunded cost associated with such a policy. The associated cost for the destruction of all unclassified hard drives (about 120,000 per year) could be significant. Current contract provides for EDS ownership of the hard drives and entitled to recovery benefits. This would be a negotiation requirement at some to-be-determined additional cost to the government. The management of hardware during the disposition process was totally revised by EDS and includes a number of safeguards and redundancies designed to prevent the release of an un-sanitized hard drive.

~~FOR OFFICIAL USE ONLY~~

This management response is not being marked "For Official Use Only" in this report.

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE  
NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL  
PROCESS (N2008-NFO000-0025.001)

Additionally, NMCI has started to deploy an NSA approved solution based on JTF-GNO direction to encrypt all unclassified hard drives at the workstation. Once encrypted, all data on the hard drive is protected while in use at the workstation level and later during the refresh process. The Data at Rest Project is scheduled for completion in CY 2009. The PEO believes that a combination of the new procedures instantiated by EDS along with the Data at Rest protection project provide a more cost effective approach to risk mitigation with respect to hard drive disposition.

Recommendation 13: Concurrent with DON CIO's, NETWARCOM's, and MCNOSC's efforts to address Recommendations 1 through 12, determine whether or not actions taken and planned require modifications to the existing NMCI contract. If so, identify the specific contract modifications that will need to be made, and initiate prompt action(s) to implement the modifications.

PEO-EIS Comment: Concur. PMW-200 will determine the contract modifications necessary to implement the approved policy changes related to recommendations 1 through 12. Actions necessary to implement the changes will be taken, and the Procuring Contract Officer will negotiate any required changes and costs with EDS.

Recommendation 14: Ensure that policy, and procedure changes resulting from Recommendations 1 through 12 are made an integral part of the Next Generation Enterprise Network (NGEN) contract and related internal controls and governance processes.

PEO-EIS Comment: Concur. PEO-EIS will work with ACNO NGEN System Program Office to integrate the changes into the contract and related internal controls and governance processes based on approved policy changes resulting from recommendations 1 through 12.

2. Please address comments or concerns to [REDACTED]

FOIA (b)(6)

Subj: PROCESSING OF COMPUTER AND HARD DRIVES DURING THE  
NAVY MARINE CORPS INTRANET (NMCI) COMPUTER DISPOSAL  
PROCESS (N2008-NFO000-0025.001)

Copy to:  
Assistant Audit for Manpower and Reserve Affairs, [REDACTED]  
Audit Director, [REDACTED]  
ASN RD&A  
ACNO NGEN SPO  
DON CIO  
OPNAV N61  
NNWC  
SEAWAR 8.6  
CMC (C4)  
PM NMCI  
PM NGEN

FOIA (b)(6)

**Use this page as**

# **BACK COVER**

**for printed copies**

**of this document**