

# Naval Audit Service



## Audit Report



### Followup on Naval Audit Service Report N2012-0009, “Personally Identifiable Information and Department of the Navy Data on Unencrypted Computer Hard Drives Released from Department of the Navy Control”

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

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

**N2015-0027**  
**23 July 2015**

## Obtaining Additional Copies

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

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

## Providing Suggestions for Future Audits

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

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

## Naval Audit Service Web Site

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

<http://www.secnav.navy.mil/navaudsvc>



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

7510  
2014-049  
23 Jul 15

**MEMORANDUM FOR DEPARTMENT OF THE NAVY CHIEF INFORMATION  
OFFICER**

**Subj: FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

**Ref:** (a) NAVAUDSVC Memorandum 7510, 2014-049 dated 19 Mar 2014  
(b) SECNAV Instruction 7510.7F, “Department of the Navy Internal Audit”  
(c) Naval Audit Service report, “Personally Identifiable Information and  
Department of the Navy Data on Unencrypted Computer Hard Drives  
Released from Department of the Navy Control,” N2012-0009, 8 Dec 2011

**Encl:** 1. Status of Recommendations  
2. Pertinent Guidance  
3. Scope and Methodology  
4. Activities Visited or Contacted  
5. Management Response from Office of the Department of the Navy Chief  
Information Officer

**1. Introduction.**

a. This report provides results of the subject audit announced in reference (a). For this report, computer hard drives refer to computer hard disk drives retired from service by the tech refresh process. Storage Area Network, Network Attached Storage, and Wide Area Network Acceleration drives were outside the scope of this audit. We found that some unencrypted computer hard drives and Naval Nuclear Propulsion Information (NNPI) hard drives were not properly handled despite process improvements implemented by the Department of the Navy Chief Information Officer (DON CIO). We also found that Navy Marine Corps Intranet’s (NMCI’s) Data at Rest encryption does not provide assurance that hard drive data is protected from unauthorized users. Therefore, this report, like our previous one, contains a recommendation that all computer hard drives be physically destroyed.

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

b. Paragraph 5 provides a summary of our audit results. Paragraph 6 provides our recommendations to the DON CIO, management responses from the Acting DON CIO, and our comments on the responses.

2. **Audit Objective and Reason for Audit.** The audit objective was to verify whether or not conditions identified in Naval Audit Service audit report N2012-0009, “Personally Identifiable Information and Department of the Navy Data on Unencrypted Computer Hard Drives Released from Department of the Navy Control,” 8 December 2011, still existed. We wanted to determine whether new DON CIO policies and procedures provided reasonable assurance that Personally Identifiable Information (PII),<sup>1</sup> sensitive DON data, and unencrypted hard drives would not be improperly released from DON custody and control.

3. **Background.** This audit is a followup to our December 2011 report [reference (c)]. Based on a limited sample of computers, the prior audit found over 240,000 Social Security numbers, other PII, and sensitive DON data on hard drives could have been inappropriately released from DON custody and control. This compromise of PII and sensitive DON data occurred because the DON CIO Message requiring the physical destruction of hard drives also permitted waivers to the physical destruction requirement. Had waivers not been approved, the condition we found would not have existed, as the hard drives containing this information would have been physically destroyed as required. At the time of our audit fieldwork, the waiver policy<sup>2</sup> had been extended through 30 May 2015. After we briefed the Acting DON CIO on the issues in this report, the waiver policy was again extended; this time through 30 June 2018.

4. **Briefings with Management.** We briefed our methodology and the status of the audit work to DON CIO on 23 April 2014. On 7 May 2014, we met with the DON CIO Compliance Branch Head and Privacy Lead and Naval Enterprise Networks Program Management Office (PMW-205)<sup>3</sup> to discuss the audit and preliminary results. We briefed our preliminary audit results to the PMW 205 Deputy Program Manager on 30 September 2014 and provided an update to the PMW 205 Product Support Manager and Asset Manager on 9 April 2015. On 17 March 2015, we briefed the Acting DON CIO.

---

<sup>1</sup> The Secretary of the Navy Instruction 5211.5E, “DON Privacy Program,” dated 28 December 2005, defines personally identifiable information (PII) as any information or characteristics that may be used to distinguish or trace an individual’s identity, such as their name, Social Security number, or biometric records.

<sup>2</sup> DON Deputy CIO Navy Memo, “Hard Disk Drive Destruction Waiver Extension,” dated 30 October 2014, extended the Program Executive Officer Enterprise Information Systems (PEO EIS) Hard Disk Drive (HDD) destruction policy waiver request until 30 May 2015

<sup>3</sup> PMW-205 reports to the Program Executive Officer, Enterprise Information Systems.

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

5. **Audit Results.** We found that DON CIO’s process improvements did not resolve our prior audit findings. We again found that not all DON computer hard drives were properly processed. We identified unencrypted computer hard drives that were not properly processed and were informed of Naval Nuclear Propulsion Information (NNPI) hard drives that were not properly handled. The improper handling of computer hard drives occurred because Navy and contractor personnel did not adhere to the Office of the Chief of Naval Operations Instructions and DON CIO’s process. Improperly processing computer hard drives increase the potential for a compromise of national security information, controlled unclassified information, and PII.

a. **Unencrypted Hard Drives.** We conducted site visits to the Hewlett Packard Enterprise Services (HPES) Warehouse<sup>4</sup> in Mechanicsburg, PA and Hewlett Packard cross-dock facility<sup>5</sup> at Andrews Air Force Base, Suitland, MD and sampled 925 of approximately 3,453 computers. Enclosure (3) contains details on the methodology. In our sample, we found 12 computer hard drives<sup>6</sup> that were not encrypted as required and, therefore, should not have been released to the contractor. In addition, we found 79 computer hard drives that were not readable.<sup>7</sup> If the computer hard drives were not readable at the time of pickup, encryption status could not be determined and, therefore, they should not have been released to the contractor. This improper processing of unencrypted computer hard drives was also identified in our prior audit report, and was not corrected as intended by the DON CIO’s process improvements; therefore, we consider this a repeat finding.

i. According to the DON CIO Message 281759Z, “Processing of Electronic Storage Media for Disposal,” dated August 2012, electronic storage media that are not encrypted must be fully documented and physically destroyed. Also, per the Continuity of Services Contract (CoSC) Work Instruction for all refresh seats that do not have data-at-rest (DAR) installed, the hard drives will be removed and turned over to the on-site Government point of contract.

b. **NNPI Hard Drives.** Mechanicsburg warehouse personnel told us that four NNPI hard drives were contained in shipments received in 2013 and one was received in 2014. These five NNPI hard drives were determined to be unclassified NNPI (U-NNPI) by the contractor. Even though they were determined to be unclassified, NNPI hard drives are prohibited from being removed from the owning Navy command and should have been

---

<sup>4</sup> The warehouse is the last processing site prior to the computers being released to resellers.

<sup>5</sup> The cross-dock facility is a site for collecting and processing computers and eventually all computers will be transported to Mechanicsburg warehouse.

<sup>6</sup> None of these 12 computer hard drives contained PII.

<sup>7</sup> Non-readable hard drives may or may not have been readable when released.

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

physically destroyed. Although we were told the five NNPI hard drives were returned to the commands from which they were removed, and that the commands then sent the hard drives to NSA to be physically destroyed, no tracking evidence supporting this was available from the contractor. If the contractor and command personnel followed existing Office of the Chief of Naval Operations Instruction and DON CIO’s process, this situation would not have occurred because the command personnel would not have released the NNPI hard drives to the contractor personnel, and, instead, would have processed them for physical destruction.

i. According to the Office of the Chief of Naval Operations (OPNAV) Instruction N9210.3, “Safeguarding of Naval Nuclear Propulsion Information (NNPI), Unclassified Portion,” dated 7 June 2010, “NNPI shall be safeguarded to prevent its disclosure to the public and others without the appropriate clearance and need-to-know. U-NNPI shall be controlled so that those without a need-to-know cannot obtain visual or physical access that would permit detailed examination. U-NNPI materials shall be purged or destroyed<sup>8</sup> before disposal or release outside of the Naval Nuclear Propulsion Program. Disposal of U-NNPI as classified material is also acceptable.” According to DON CIO Message 281759Z, classified, unclassified Naval Criminal Investigative Service (NCIS), and U-NNPI electronic storage media are not eligible for a waiver and should be physically destroyed. The CoSC Work Instruction stated “NNPI, NCIS, and SIPR [Secret Internet Protocol Router] seats MUST have hard drives removed at site and turned over to the Government with appropriate DD250 recorded.”

c. **Decryption.** We found that NMCI’s Data at Rest encryption does not provide assurance that hard drive data is protected from unauthorized users. We provided two DON hard drives with Data at Rest encryption from our sample to NCIS and requested that they attempt to breach the encryption. NCIS was able to decrypt both of the hard drives using what they described as off-the-shelf forensic software available to others. NCIS personnel stated that DON hard drives with Data at Rest encryption could be decrypted by others outside DON given the proper resources. Once the encrypted hard drives were decrypted, auditors were able to access all information, including PII, on the hard drives without using any special software or skills. For these reasons, along with the previously discussed process control failures to follow required procedures, we continue to believe that in the interest of our national security and in minimizing the risk of inappropriately releasing PII, all DON computer hard drives, to include those with Data at Rest encryption, should be physically destroyed, and not be eligible for a destruction waiver.

---

<sup>8</sup> National Institute of Standards and Technology (NIST) Special Publication 800-88 of September 2006, Guidelines for Media Sanitization.

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

6. **Recommendations and Corrective Actions.** Our recommendations are below, along with summarized management responses to the overall report and each recommendation, and our comments on the responses. The complete text of management’s response is in Enclosure 5.

**Department of the Navy Chief Information Officer (DON CIO) General Response to the Report.** In their official response to our draft report, the Acting DON CIO states that “the DON CIO fully supports the physical destruction of magnetic hard disk drives (HDDs) at the end of their services lives, and has implemented guidance directing it. Under the Next Generation Enterprise Network (NGEN) contract, computer HDDs retired from service by tech refresh, including those subject to previous waivers, are physically destroyed.” DON CIO also states that the waiver (DON CIO Message 281759Z) applies only to failed Storage Area Network (SAN), Network Attached Storage (NAS), and Wide Area Network Acceleration (WANX) drives.

**Naval Audit Service Comment on DON CIO General Response.** The Acting DON CIO’s response<sup>9</sup> states that they have implemented guidance directing the physical destruction of magnetic hard disk drives. If properly implemented, along with Recommendation 3 to rescind or revise DON CIO Message 281759Z so that future waivers to the physical destruction of computer hard drives will not be permitted, the overall intent of all of our recommendations could be satisfied. However, contrary to DON CIO’s response, the language in the waiver – which DON CIO has extended to 30 June 2018 – does not specify that the waiver only applies to SAN, NAS, and WANX drives (none of which were within the scope of this audit). Therefore, the risk remains that computer hard drives will not be physically destroyed.

We recommend that the Department of the Navy Chief Information Officer (DON CIO):

**Recommendation 1.** Require that all computer hard drives be physically destroyed.

**Management response to Recommendation 1.** Nonconcur. Naval Enterprise Networks Program Management Office (PMW-205) estimates that only 440 failed drives per year come under the waiver. Failed SAN, NAS, and WANX drives must be returned to the original equipment manufacturer as part of a maintenance agreement. Repairable drives are placed back into service. Drives that are not repairable are physically destroyed. However, it is DON policy that all Storage

---

<sup>9</sup> The official management responses were signed out by the Acting DON CIO. Subsequently, a permanent new DON CIO was appointed.

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

Area Network/Network Attached Storage and Wide Area Network Acceleration drives are physically destroyed at the end of their service life.

**Naval Audit Service comment on the response to Recommendation 1.** The Acting DON CIO’s response did not address our recommendation that all computer hard drives be physically destroyed. Instead, the Acting DON CIO’s response provided a rationale for not destroying certain types of hard drives (i.e., SAN, NAS, and WANX drives) which were not within the scope of this audit. Since the Acting DON CIO’s response did not address the physical destruction of the desktop, laptop, and notebook computer hard drives that were the subject of this audit, we consider this recommendation to be undecided, and are resubmitting it to the (new) DON CIO for reconsideration. If the new DON CIO also nonconcur with this recommendation, or if a response is not provided within 30 days of this report, the recommendation will be elevated to his immediate superior.

**Recommendation 2.** Do not extend the computer hard drives waiver provision of the Department of the Navy Chief Information Officer Message 281759Z when the waiver expires 30 May 2015.

**Management response to Recommendation 2.** Nonconcur. The risk of unauthorized disclosure of Controlled Unclassified Information is very low. SAN and NAS infrastructure incorporate redundant array of independent disks technology. As such, the data is split into blocks and distributed across an array of drives. Data is logically sequential, so with consecutive segments stored on different physical storage devices, it is not possible to reassemble data from a single disk. PMW 205 recently tested three SAN drives and confirmed that there were no data remnants and no imaging was possible. According to PMW 205, the results would be similar for NAS drives. Data written to the hard drive of a WANX appliance is scrambled and is not readable using Salable Data Referencing technology. PMW 205 tested and confirmed that no WANX data was readable.

**Naval Audit Service comment on the response to Recommendation 2.** After issuing a draft of this report, we learned that on 23 March 2015, the DON Deputy Chief Information Officer (Navy) extended waiver provision of the DON CIO Message 281759Z until 30 June 2018. Furthermore, the language in the waiver does not specify that the waiver only applies to SAN, NAS, and WANX drives (none of which were within the scope of this audit). Therefore, we consider this recommendation to be undecided, and are resubmitting it to the new DON CIO for reconsideration. If the new DON CIO also nonconcur

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

with this recommendation, or if a response is not provided within 30 days of this report, the recommendation will be elevated to his immediate superior.

**Recommendation 3.** Rescind or revise Department of the Navy Chief Information Officer Message 281759Z so that future waivers to the physical destruction of computer hard drives will not be permitted.

**Management response to Recommendation 3.** Nonconcur. The cost to the Government is unacceptably high without this waiver. The DON retains failed hard disk drives rather than returning them to the original equipment manufacturer. That is a maintenance issue not covered by the Next Generation Enterprise Network contract. Therefore, the DON is charged a fee for each retained disk. PMW 205 estimates that the cost to the DON would be approximately \$600K per year without the waiver.

**Naval Audit Service comment on the response to Recommendation 3.** The Acting DON CIO’s response did not address our recommendation to rescind or revise DON CIO Message 281759Z. Instead, the Acting DON CIO’s response provided a rationale for the cost of retaining failed hard drives other than those within the scope of this audit. Since the Acting DON CIO’s response did not address not permitting future waivers to the physical destruction of desktop, laptop, and notebook computer hard drives that were the subject of this audit, we consider this recommendation to be undecided and we are resubmitting it to the new DON CIO for reconsideration. If the new DON CIO also nonconcur with this recommendation, or if a response is not provided within 30 days of this report, the recommendation will be elevated to his immediate superior.

**Recommendation 4.** Notify Navy and Marine Corps Commands, and contractor personnel of the changes made to require the physical destruction of computer hard drives in all instances.

**Management response to Recommendation 4.** Nonconcurrency is based on the rationales for Recommendations 1-3.

**Naval Audit Service comment on the response to Recommendation 4.** Because we are resubmitting Recommendations 1, 2, and 3 to the new DON CIO for reconsideration, we are also resubmitting this recommendation for reconsideration. If the new DON CIO also nonconcur with this recommendation, or if a response is not provided within 30 days of this report, the recommendation will be elevated to his immediate superior.

**FOR OFFICIAL USE ONLY**

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

**Other Management Responses and Naval Audit Service Comments.** The Acting DON CIO nonconcurred with our finding that NMCI’s Data at Rest encryption does not provide assurance that hard drive data is protected from unauthorized users. As described in this report, NCIS was able to decrypt both of the hard drives using what they described as off-the-shelf forensic software available to others. NCIS personnel stated that DON hard drives with Data at Rest encryption could be decrypted by others outside DON given the proper resources. In our judgment, this poses an unacceptable risk of unauthorized access to information on disposed-of hard drives. Therefore, we continue to believe that the physical destruction of desktop, laptop, and notebook computer hard drives recommended in this report and our prior report provides the most assurance that DON data will be protected from unauthorized users.

**7. Other Information.**

a. Management did not concur with Recommendations 1 through 4; therefore, the recommendations are considered undecided and are being resubmitted to the DON CIO for reconsideration. DON CIO is required to provide comments on the undecided recommendations within 30 days. If the new DON CIO also nonconcurs with this recommendation, or if a response is not provided within 30 days of this report, the recommendation will be elevated to his immediate superior. Please provide all correspondence to XXXXXXXXXXXXXXXX, Assistant Auditor General for Manpower and Reserve Affairs Audits by e-mail at XXXXXXXXXXXXXXXX, with copies to XXXXXXXXXXXXXXXX, Audit Director, XXXXXXXXXXXXXXXX, as well as the Director, Policy and Oversight, XXXXXXXXXXXXXXXX and the Naval Audit Service Followup Coordinator, XXXXXXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)

FOIA (b)(6)

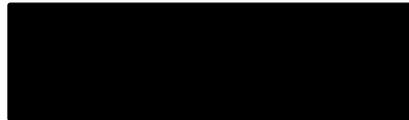
FOIA (b)(6)

b. In order to protect privacy and other sensitive information included in this report, we request that you do not release this report outside the Department of the Navy, post on non-Naval Audit Service Web sites, or in Navy Taskers without the prior approval of the Auditor General of the Navy.

**FOR OFFICIAL USE ONLY**

Subj: **FOLLOWUP ON NAVAL AUDIT SERVICE REPORT N2012-0009,  
“PERSONALLY IDENTIFIABLE INFORMATION AND DEPARTMENT  
OF THE NAVY DATA ON UNENCRYPTED COMPUTER HARD DRIVES  
RELEASED FROM DEPARTMENT OF THE NAVY CONTROL”  
(AUDIT REPORT N2015-0027)**

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



FOIA (b)(6)

XXXXXXXXXXXXXXXXXXXX  
Assistant Auditor General  
Manpower and Reserve Affairs Audits

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

**Enclosure 1:****Status of Recommendations**

Recommendations							
Finding <sup>10</sup>	Rec. No.	Page No.	Subject	Status <sup>11</sup>	Action Command	Target or Actual Completion Date	Interim Target Completion Date <sup>12</sup>
+1	1	5	Require that all computer hard drives be physically destroyed.	U	Department of the Navy Chief Information Officer	8/24/15	
+1	2	6	Do not extend the computer hard drives waiver provision of the Department of the Navy Chief Information Officer Message 281759Z when the waiver expires 30 May 2015.	U	Department of the Navy Chief Information Officer	8/24/15	
+1	3	7	Rescind or revise Department of the Navy Chief Information Officer Message 281759Z so that future waivers to the physical destruction of computer hard drives will not be permitted.	U	Department of the Navy Chief Information Officer	8/24/15	
+1	4	7	Notify Navy and Marine Corps Commands, and contractor personnel of the changes made to require the physical destruction of computer hard drives in all instances.	U	Department of the Navy Chief Information Officer	8/24/15	

<sup>10</sup> / + = Indicates repeat finding.

<sup>11</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.

<sup>12</sup> If applicable.

## **Pertinent Guidance**

**Secretary of the Navy Instruction 5211.5E, “DON [Department of the Navy] Privacy Program,”** dated 28 December 2005, defined personally identifiable information as any information or characteristics that may be used to distinguish or trace an individual’s identity, such as their name, Social Security number, or biometric records.

**Office of the Chief of Naval Operations Instruction N9210.3, “Safeguarding of Naval Nuclear Propulsion Information (NNPI),”** dated 7 June 2010, defined NNPI as classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of Naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. NNPI shall be safeguarded to prevent its disclosure to the public and others without the appropriate clearance and need-to-know. Unclassified-NNPI (U-NNPI) shall be controlled so that those without a need-to-know cannot obtain visual or physical access that would permit detailed examination. U-NNPI materials shall be purged or destroyed<sup>13</sup> before disposal or release outside of the Naval Nuclear Propulsion Program. Disposal of U-NNPI as classified material is also acceptable.

**DON Chief Information Officer (DON CIO) Message 281759Z, “Processing of Electronic Storage Media for Disposal,”** dated August 2012, stated that physical destruction occurs when the electronic storage device or media is made inoperable and unrecoverable through shredding, crushing, burning, or melting. All DON-owned, leased, or purchased electronic storage media and information systems shall remain in DON custody and control until physically destroyed in accordance with references E<sup>14</sup> and F<sup>15</sup> unless shipped to the National Security Agency (NSA). Classified, unclassified Naval Criminal Investigative Service (NCIS), and U-NNPI electronic storage media are not eligible for a waiver. Waivers from the destruction requirement for unclassified electronic storage media may be requested from the DON Deputy CIO (Navy) or DON Deputy CIO (Marine Corps), provided the following conditions are met: electronic storage media is encrypted with a DON approved Data at Rest solution and is individually tested to verify no data is readable while still in DON possession and prior to shipment to approved facility for disposal; and the host network has implemented full disk and electronic storage media encryption across the network. Electronic storage media that are not encrypted must be fully documented and physically destroyed.

---

<sup>13</sup> National Institute of Standards and Technology (NIST) Special Publication 800-88 of September 2006, “Guidelines for Media Sanitization.”

<sup>14</sup> NIST September 2006.

<sup>15</sup> Committee on National Security Systems August 2006.

**DON Deputy CIO Navy Memo, “Hard Disk Drive Destruction Waiver Extension,”** dated 31 October 2014, stated that reference (b)<sup>16</sup> approved the Program Executive Officer Enterprise Information Systems (PEO EIS) Hard Disk Drive (HDD) destruction policy waiver request until 30 April 2014 and reference (c)<sup>17</sup> extended the PEO EIS HDD destruction policy waiver request until 30 November 2014. This memorandum hereby extended the waiver for HDD Destruction until 30 May 2015 to allow for Next Generation Enterprises Network (NGEN) implementation.

On 23 March 2015, DON Deputy CIO extended the waiver to 30 June 2018.

**NGEN Contract**, 1 October 2014, requires the disposal of classified and unclassified hard drives, in accordance with DON CIO Message Processing of Electronic Storage Media for Disposal 281759Z 12 August 2012.

**Navy Telecommunications Directive 03-11, “Disposal of Navy Computer Hard Drives,”** dated 2 May 2011, stated all hard drives that have been used in Navy classified or unclassified networks are the property of the Navy, specifically the command to which users of that hard drive are assigned, and shall be the responsibility of that command. Commands may request a DON Deputy CIO Navy waiver from this destruction requirement in cases that an approved Data at Rest solution with full disk encryption has been implemented. Unclassified hard drives with approved waivers may be turned over to a Navy/Marine Corps Intranet primary contractor or other service contract vendors. All commands are subject to inspections by appropriate authorities to ensure compliance (e.g., Naval Audit Service).

---

<sup>16</sup> DON Deputy CIO Washington DC letter of 6 February 2012.

<sup>17</sup> DON Deputy CIO Washington DC letter of 1 May 2014.

## Enclosure 3:

# Scope and Methodology

We performed this followup audit on personally identifiable information and Department of the Navy (DON) data on unencrypted computer hard drives released from DON control from 19 March to 15 April 2015. We conducted this 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. We did not use any computer-generated data; therefore, testing the reliability of the data was not necessary.

We visited and conducted testing of computer hard drives at two locations: the Hewlett Packard Enterprise Services Warehouse, Mechanicsburg, PA, which is the final processing site prior to the computers being released to resellers; and the cross-dock at Andrews Air Force Base, Suitland, MD, which is a collecting and processing site (from which eventually all computers will be transported to the Mechanicsburg warehouse). We determined whether computer hard drives were encrypted with encryption software. For the computer hard drives that were unencrypted, we determined whether the hard drive contained readily accessible personally identifiable information.

At Mechanicsburg, we sampled a total of 261 out of 1,411 computers. We sampled 136 computer hard drives out of 891 computers from the quarantine cage and 125 computer hard drives out of 520 computers for the computers pending shipment to the resellers. Furthermore, we collected 313 stand-alone computer hard drives, which were taken back to our Washington, DC office for testing. In addition, we interviewed warehouse personnel and obtained the warehouse procedures of processing the computers from receiving the computers to shipping the computers to the resellers. We were informed of five Naval Nuclear Propulsion Information computer hard drives received by Hewlett Packard in 2013 and 2014. We followed up and obtained additional information from DON Chief Information Officer (CIO) and PMW [Program Management Office] 205.

In addition, at Andrews Air Force Base, Suitland, MD, we sampled a total of 351 out of 1,729 computers. We sampled 89 computer hard drives out of 138 computers in the quarantine cage and 132 computer hard drives out of 954 computers for the computers pending shipment to the resellers. In addition, we sampled 130 computer hard drives out of 637 computers awaiting the inventory list.

The sample size for each group was selected in order to provide a very high chance of detecting errors that occur in two percent or more of the target universe. The samples

were pulled using a combination of systematic and availability sampling. We first separated our sample based on the number of piles within the universe. For example, if there were 10 piles for a sample of 70 computers, then we would have pulled 7 computers from each pile. Desktop computers were then selected in a predetermined fashion from the top of each pile and laptop computers were selected from the corners of each box.

We obtained and analyzed the DON CIO Computer Hard Drive Disposal Plan. We held discussions with DON CIO, his staff, and PMW 205 to determine the adequacy of administration and processing controls.

**Federal Managers' Financial Integrity Act.** The Federal Managers' Financial Integrity Act (FMFIA) of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. In our opinion, the conditions noted in this report may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

**Enclosure 4:**

# **Activities Visited or Contacted**

---

- Department of the Navy Chief Information Officer, Arlington, VA\*
- Program Management Office (PMW 205), Washington Navy Yard, Washington, DC\*
- Hewlett Packard Enterprise Services (HPES) Warehouse, Naval Support Activity Mechanicsburg, Mechanicsburg, PA\*
- HPES Cross Dock, Andrews Air Force Base, Suitland, MD\*
- Naval Supply Systems Command Weapon Systems Support, Mechanicsburg, PA
- National Security Agency, Classified Material Conversion Center, Silver Spring, MD
- Naval Criminal Investigative Service, Quantico, VA and New Orleans, LA
- Department of Justice, Automated Litigation Support, Washington, DC

\* Denotes activities visited

Enclosure 5:

# Management Response from the Office of the Department of the Navy Chief Information Officer



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

18 May 2015

MEMORANDUM FOR ASSISTANT AUDITOR GENERAL OF THE NAVY FOR  
MANPOWER AND RESERVE AFFAIRS AUDITS

Subj: RESPONSE TO NAVAUDSVC FOLLOWUP REPORT N2012-0009, 15 APR 2015, PII  
AND DON DATA ON COMPUTER HARD DRIVES RELEASED FROM DON  
CONTROL

Ref: (a) NAVAUDSVC Memo to DON CIO, 7510 N2014-049, of 15 Apr 2015  
(b) DON CIO Washington DC Msg 281759Z AUG 12  
(c) OPNAV N2/N6 ltr 3000 N2N6BC/SU120060, of 23 Mar 2015

The Department of the Navy Chief Information Officer (DON CIO) has evaluated the findings and recommendations contained in reference (a). For the reasons summarized below, the DON CIO non-concurs with all four recommendations and a significant finding concerning Data at Rest (DAR) encryption.

The DON CIO fully supports the physical destruction of magnetic hard disk drives (HDDs) at the end of their service lives, and has implemented guidance directing it. Under the Next Generation Enterprise Network (NGEN) contract, computer HDDs retired from service by tech refresh, including those subject to previous waivers, are physically destroyed.

There are limited situations in which the cost of HDD destruction outweighs the risk of harm to DON personnel. For this reason, the waiver provision contained in reference (b) is a valid exception to policy. The waiver, reference (c), applies only to failed Storage Area Network (SAN), Network Attached Storage (NAS) and Wide Area Network Acceleration (WANX) drives, a relatively small number of HDDs.

Detailed rationale for non-concurrence on all four audit recommendations follows:

**Recommendation 1.** Require that all computer hard drives be physically destroyed.

**The number of HDDs covered by the waiver is very limited.** PMW 205 estimates that only 440 failed drives per year come under the waiver. Failed SAN, NAS and WANX drives must be returned to the original equipment manufacturer (OEM) as part of a maintenance agreement. Repairable drives are placed back into service. Drives that are not repairable are physically destroyed. However, it is DON policy that all SAN/NAS and WANX drives are physically destroyed at the end of their service life.

**Recommendation 2.** Do not extend the computer hard drives waiver provision of the Department of the Navy Chief Information Officer Message 281759Z when the waiver expires 30 May 2015.

Subj: RESPONSE TO NAVAUDSVC FOLLOWUP REPORT N2012-0009, 15 APR 2015, PII  
AND DON DATA ON COMPUTER HARD DRIVES RELEASED FROM DON  
CONTROL

**The risk of unauthorized disclosure of Controlled Unclassified Information (CUI) is very low.** SAN and NAS infrastructure incorporate redundant array of independent disks (RAID) technology. As such, the data is split into blocks and distributed across an array of drives. Data is logically sequential, so with consecutive segments stored on different physical storage devices, it is not possible to reassemble data from a single disk. PMW 205 recently tested three SAN drives and confirmed that there were no data remnants and no imaging was possible. According to PMW 205, the results would be similar for NAS drives. Data written to the hard drive of a WANX appliance is scrambled and is not readable using Scalable Data Referencing (SDR) technology. PMW 205 tested and confirmed that no WANX data was readable.

**Recommendation 3.** Rescind or revise Department of the Navy Chief Information Officer Message 281759Z so that future waivers to the physical destruction of computer hard drives will not be permitted.

**The cost to the government is unacceptably high without this waiver.** The DON retains failed HDDs rather than returning them to the OEM. That is a maintenance issue not covered by the NGEN contract. Therefore, the DON is charged a fee for each retained disk. PMW 205 estimates that the cost to the DON would be approximately \$600K per year without the waiver.

**Recommendation 4.** Notify Navy and Marine Corps Commands, and contractor personnel of the changes made to require the physical destruction of computer hard drives in all instances.

Non-concurrence is based on the rationales for 1 – 3 above.

**Significant Finding on Decryption.** Rationale for non-concurrence of the significant audit finding regarding DAR encryption:

Paragraph 5. c. of reference (a) states that “NMCI’s Data at Rest (DAR) encryption does not provide assurance that hard drive data is protected from unauthorized users.” Reference (a) also states that, “NCIS was able to decrypt both of the hard drives using what they described as off-the-shelf software available to others.” If these statements were accurate, it would mean that the National Institute of Standards and Technology (NIST) standards used to test, evaluate and select DAR software for the Federal Government were invalid. Actually, NCIS was only able to decrypt the hard drives using the public key of the encryption certificate and the password, not simply with off-the-shelf software. Encryption certificates are strictly controlled by the SPAWAR Systems Center-Atlantic Public Key Infrastructure Group and change every three years. By design, a DAR-enabled drive cannot be decrypted without a valid encryption certificate and password.

**FOR OFFICIAL USE ONLY**

ENCLOSURE 5: MANAGEMENT RESPONSE FROM THE OFFICE OF THE DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

---

Subj: RESPONSE TO NAVAUDSVC FOLLOWUP REPORT N2012-0009, 15 APR 2015, PII AND DON DATA ON COMPUTER HARD DRIVES RELEASED FROM DON CONTROL

Therefore, DON CIO recommends that the Naval Audit Service make the following adjustments to paragraph 5. c. of reference (a):

1. Delete the sentence stating that DAR encryption does not provide assurance that data is protected from unauthorized users.
2. Revise the statement about decryption to read, "NCIS forensics personnel were able to decrypt both of the drives using a public key of the encryption certificate and password provided by SSC-LANT and what NCIS described as off-the-shelf software."

The DON CIO will continue to work with DON stakeholders to ensure that the NGEN network maintains the highest security posture.

  
Acting

FOIA (b)(6)

Copy to:  
AUDGEN  
PEO EIS  
OPNAV N2/N6  
HQMC C4

~~FOR OFFICIAL USE ONLY~~

Use this page as  
**BACK COVER**  
for printed copies  
of this report

~~FOR OFFICIAL USE ONLY~~