

Naval Audit Service



Audit Report



Managing Personally Identifiable Information on Selected Commander, U.S. Fleet Forces Command Ships

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

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

N2015-0003
31 October 2014

Obtaining Additional Copies

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

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

Providing Suggestions for Future Audits

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

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

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
2013-025
31 Oct 14

MEMORANDUM FOR COMMANDER, U.S. FLEET FORCES COMMAND
COMMANDER, NAVAL SURFACE FORCE ATLANTIC
COMMANDER, NAVAL AIR FORCE ATLANTIC

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Ref: (a) NAVAUDSVC memo 7510 2013-025, dated 24 Jul 13
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

Encl: 1. Status of Recommendations
2. Pertinent Guidance
3. Scope and Methodology
4. Activities Visited
5. Management Response from Commander, U.S. Fleet Forces Command
6. Management Response from Commander, Naval Surface Force Atlantic
7. Management Response from Commander, Naval Air Force Atlantic

1. **Introduction.** We have completed the subject audit announced in reference (a). Paragraph 7 provides a summary of audit results. We found internal control weaknesses over the protection of personally identifiable information (PII) that we considered to be material. However, the audit found opportunities to improve those conditions by providing oversight and through implementation of the recommendations presented in paragraph 9. Management responded to the recommendations by taking and/or planning appropriate corrective actions.

2. **Reason for Audit.** The audit objective was to verify that internal controls over PII on selected Commander, U.S. Fleet Forces Command (CFFC) ships are in place and operating effectively to protect information from unauthorized disclosure. This audit specifically focused on Commander, Naval Surface Force Atlantic (COMNAVSURFLANT) and Commander, Naval Air Force Atlantic (COMNAVAIRLANT) ships. We conducted this audit because PII was identified as high risk by the Department of the Navy (DON) Chief Information Officer (CIO) in the

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Fiscal Year (FY) 2013 annual risk assessment. This is one of a series of audit efforts to address management of PII within DON.

3. Background.

a. FFC's mission is to train, certify, and provide combat-ready Navy forces to Combatant Commanders that are capable of conducting prompt, sustained Naval, joint, and combined operations in support of U.S. national interests. FFC directs and controls subordinate Navy forces and shore activities during the planning and execution of assigned service functions in support of the Chief of Naval Operations. The Command also provides operational planning and coordination support to Commander, U.S. Northern Command; Commander, U.S. Element North American Aerospace Defense Command; and Commander, U.S. Strategic Command.

b. The Privacy Act of 1974 established requirements for Federal agencies maintaining information in a system of records. The Department of Defense's (DoD's) determination of a system of records is a group of records under the control of a DoD component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifier assigned to an individual. This type of information was previously called "Privacy Act information" and "protected personal information." It is now referred to as PII.

c. In recent years, DON has experienced repeated inadvertent releases of PII of Navy and Marine Corps military and civilian personnel and their dependents. The primary cause of these events is mishandling of PII due to human error. Insider threats, whereby PII is willfully stolen or compromised, happen with low frequency, but are becoming a growing trend. While cases of verifiable identity theft to DON personnel have been low, the potential for widespread fraud is considered a high risk. Changes to policy, increased PII awareness, and technology solutions have improved the security and handling of PII. However, personal and command accountability have been considered insufficient.

d. Proper handling of PII will mitigate DON administrative costs and time spent rectifying breaches. Moreover, reducing the loss of PII will improve Sailor and Marine morale, and command and DON reputation, as well as decrease the likelihood of identity theft and financial fraud to personnel Navy-wide.

4. Briefings with Management. Our opening conference with FFC and COMNAVSURFLANT occurred on 14 August 2013. An additional opening conference with COMNAVAILANT occurred on 20 August 2013. We kept the commands apprised of our review progress throughout the audit. The closing conference was held on 24 March 2014.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

5. Noteworthy Accomplishments. We noted that the *USS GEORGE H.W. BUSH* (CVN 77) had areas of strength within their Privacy Act program. The *USS GEORGE H.W. BUSH* established:

- Guidance, *USS GEORGE H.W. BUSH* (CVN 77) Instruction 5211.1A, for the execution and maintenance of an onboard Privacy Act program;
- A command Privacy Act Coordinator (PAC);
- A Privacy Act team; and
- Monthly spot checks on a rotational basis so that each department is assessed at a minimum of one time per calendar year.

6. Federal Managers' Financial Integrity Act (FMFIA) of 1982. This Act, 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 1-19 address issues related to the internal control weaknesses in the use, collection, safeguarding, disposal, and Web site content of PII. In our opinion, the internal control weaknesses noted in this report are significant issues of noncompliance with the DON Privacy Act Program and could potentially result in the compromise of PII. We believe this audit and others show that insufficient controls over PII in DON is a systemic weakness that may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

7. Audit Results. We examined PII internal controls onboard four COMNAVSURFLANT ships (*USS GONZALEZ*, *USS GUNSTON HALL*, *USS NITZE*, and *USS NORMANDY*) and one COMNAV AIRLANT ship (*USS GEORGE H.W. BUSH*) through analyses, interviews, and reviews of appropriate documentation and information systems. Internal control weaknesses were found in the following areas:

- DON Privacy Program implementation;
- Semiannual PII spot checks;
- Disposal methods;
- PII training;
- Safeguarding PII;
- Privacy Act Statements on locally generated forms;
- Publically accessible Web sites; and
- Managers' Internal Control program.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

These conditions generally occurred because (1) there was insufficient monitoring and oversight of the Privacy Act program, and (2) DON guidance was not fully implemented. When internal controls are not properly implemented and executed, there is an increased risk of information compromise and limited ability to plan for and respond to unintended releases, breaches, or unauthorized disclosures. This could result in identity theft or fraud, which would have a negative impact on the ships, DON, and the individuals whose PII is compromised. This audit was conducted from 14 August 2013 through 26 August 2014. The pertinent guidance used during this audit is identified in Enclosure 2. The scope and methodology used for this audit are discussed in Enclosure 3. Enclosure 4 includes the activities visited.

a. DON Privacy Program Implementation.

(1) At the time of our audit, COMNAVSURFLANT did not have a Privacy Act program in place for the ships within its command in accordance with Secretary of the Navy (SECNAV) Instruction 5211.5E. COMNAVAIRLANT has a Privacy Act program, but it needs improvement; the ship we visited did not receive sufficient oversight of internal controls to mitigate the risk of unauthorized disclosure of PII or to protect the confidentiality of records containing this information.

(2) COMNAVSURFLANT and COMNAVAIRLANT did not conduct and document staff assistance visits to the ships, as required. Specifically, SECNAV Instruction 5211.5E states that Privacy Act Coordinators at Navy Echelon II and III commands will conduct and document staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the Privacy Act. COMNAVSURFLANT, COMNAVAIRLANT, and their ships were unaware of the SECNAV Instruction 5211.5E requirements.

b. Semiannual PII Spot Checks. The COMNAVSURFLANT ships reviewed did not conduct and document semiannual PII spot checks as required by SECNAV Message 042232Z of October 2007. This policy requires commanding officers to ensure that supervisors conduct and document spot checks of their assigned areas of responsibility, focusing on those areas that deal with PII on a regular basis.

c. Disposal Methods. Disposal methods on four ships were insufficient to render PII unrecognizable or beyond reconstruction, as required by SECNAV Instruction 5211.5E. During site visits we reviewed 27 shredders and found that 5 did not render PII unrecognizable or beyond reconstruction. For example, we found recognizable sensitive PII disposed in trash cans aboard the *USS GUNSTON HALL*. Documents found had PII, including the names, phone numbers, and the last four digits of Social Security numbers (SSN) for Sailors; and forms also had PII, such as names, phone numbers, and full SSN.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

d. **PII Training.** Mandated FY 2013 PII training was incomplete for the *USS Nitze*. Although ship personnel verbally stated that training was completed, they did not have sufficient documentation to verify that personnel had completed FY 2013 PII training. DON CIO Message 181905Z of December 2008 requires all personnel to complete PII training annually.

e. **Safeguarding PII.** Safeguarding PII was not fully accomplished at the five ships visited. SECNAV Instruction 5211.5E states that DON activities are responsible for establishing appropriate administrative, technical, and physical safeguards to ensure that the documents in every system of records are protected from unauthorized alteration or disclosure. They are also responsible for ensuring that confidentiality is protected. In addition, DON CIO Message 171952Z of April 2007 requires all documents containing PII to be marked “FOR OFFICIAL USE ONLY PRIVACY SENSITIVE ANY MISUSE OR UNAUTHORIZED DISCLOSURE CAN RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.”

(1) **Physical Safeguarding.** We found unsecured PII on all five FFC ships visited. According to SECNAV Instruction 5211.5E, DON activities are responsible for protecting PII from being widely disseminated. They are also responsible for ensuring that access and disclosure of PII is strictly limited to individuals with an official need to know. We found 232 unsecured PII documents in 16 of the 38 departments reviewed. In addition, we found another 39 PII documents that did not include the required “For Official Use Only” statement.

(a) On the *USS GONZALEZ*, we found 100 unsecured PII documents¹ in 5 of the 7 departments and one unlocked unit containing unsecured PII documents. There were five PII documents that did not include the appropriate “For Official Use Only” statement.

(b) On the *USS GUNSTON HALL*, we found 65 unsecured PII documents (i.e., Career Counselor Divisional binder, Leave Request Authorization forms, muster reports, and Immediate Reenlistment Agreement forms) in 3 of 6 departments. There were nine PII documents that did not include the required “For Official Use Only” statement.

(c) On the *USS NITZE*, we found an unlocked file cabinet containing 38 documents that had unsecured PII. The personal information included name, rank, full SSN, and home and work telephone numbers. There were four PII documents that did not include the required “For Official Use Only” statement.

¹ These included Special Request/Authorization, Evaluation Report and Counseling Records (E1 – E6), Immediate Reenlistment Agreement, Ready Reserve Transfer Request Service Agreement, Service Member Career Readiness Standards/Individual Transition Plan Checklist, Preparation Counseling Checklist, Leave Request/Authorization, Travel Authorization, and Fitness and Counseling Record.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

(d) On the *USS NORMANDY*, we found six unsecured PII documents (i.e., a binder with designation of authority letters and loose documentation located in unsecured overhead storage, which contained the last four numbers of Sailors' SSNs) in 3 of the 7 departments. There were three PII documents on one ship that did not contain the required "For Official Use Only" statement.

(e) On the *USS GEORGE H.W. BUSH*, we found 23 unsecured PII documents in 4 of 11 departments. There were 18 PII documents that did not include the required "For Official Use Only" statement.

(2) **Electronic Safeguarding.** Computers were reviewed to determine whether (1) e-mails containing PII were encrypted, and (2) there were sufficient controls and permissions over shared drives. DON CIO Message 32009Z of October 2008 states that users must digitally sign e-mail messages requiring either message integrity and/or non-repudiation, and encrypt messages containing sensitive information. DON CIO Message 201839Z of November 2008 states that command leadership must ensure that proper controls and permissions are in place to safeguard data on a shared drive. We found instances where computers at four ships did not have sufficient safeguards. In total, we examined 148 e-mails at four ships (*USS GUNSTON HALL*, *USS NITZE*, *USS NORMANDY*, and *USS GEORGE H.W. BUSH*) and found that:

(a) Five of 148 e-mails on three ships (*USS NITZE*, *USS NORMANDY*, and *USS GEORGE H.W. BUSH*) included PII, and 3 e-mails were not encrypted.

(b) Shared network drives on the four ships did not have proper access controls in place to safeguard data being stored on the drives. We found 12 network folders that did not restrict access, thus allowing unfettered access to restricted information to persons without a need to know. We also found 24 PII documents on these shared network drives.

f. **Privacy Act Statements on Locally Developed Forms.** We examined forms developed locally on the ships. The forms collected information that is considered PII (i.e., name with rate, SSN (in whole or in part), and date of birth). These forms were not marked with a Privacy Act statement as required by SECNAV Instruction 5211.5E, which has explicit requirements for collecting PII from an individual. Additionally, SECNAV Instruction 5210.16 requires that forms and information collection that solicit personal information shall be cleared through Chief of Naval Operations (DNS-36) to ensure that a Privacy Act System of Records Notice permitting such collection exists. However, not all ship forms used to collect PII had an indication that they were cleared through DNS-36.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

g. **Publicly Accessible Web sites.** We examined the official navy.mil Web sites of FFC, COMNAVSURFLANT, COMNAVAIRLANT, and the five selected ships. We reviewed the related official social media Web sites for PII content.

(1) We found that 9 of 40 leadership biographies did not follow the requirements for publicly accessible Web sites found in SECNAV Instruction 5720.44C. Specifically:

(a) Eight biographies included the place of birth. According to SECNAV Instruction 5720.44C, place of birth, if desired to be included, will be presented as "...is a native of..."

(b) Three biographies included family information. SECNAV Instruction 5720.44C, states that biographies published on publicly accessible Web sites will not include any information about family members.

(2) We identified 7 webmasters for the sites reviewed. Four of the 7 had the Public Affairs Officer functions as collateral duties, and only two had formal training in this area. This occurred due to insufficient periodic public affairs function training and non-compliance with SECNAV Instruction 5720.44C. Through training, Webmasters receive the knowledge necessary for ensuring that biographies comply with SECNAV guidance to prevent the unauthorized disclosure of PII. The loss or unauthorized disclosure of PII may result in substantial harm and inconvenience to the individuals affected.

h. Managers' Internal Control Program.

(1) We found that a Managers' Internal Control (MIC) Program had not been established on the COMNAVSURFLANT ships that we visited as required by SECNAV Instruction 5200.35E² and COMNAVSURFLANT Notice 5200.1. PII was not included as an assessable unit under the FY 2012 and 2013 MIC programs, nor had PII been subject to an evaluation at COMNAVSURFLANT since February 2009. Further, supporting documentation was not available to validate that internal controls were implemented to provide reasonable assurance that the following objectives were met: (1) effectiveness and efficiency of operation; (2) reliability of financial reporting; and (3) compliance with applicable laws, as reported on the annual Statements of Assurance for 10 COMNAVAIRLANT activities for FY 2013. Supporting documentation was not provided because the reporting activities are not required to submit documentation with the Statements of Assurance filed. Additionally, the nature of ship operations necessitates the collection and management of PII for Sailors onboard. PII collected on

² Subsequent to audit field work the SECNAV Instruction was updated to SECNAV Instruction 5200.35F, dated 21 July 2014. An analysis of the wording shows changes with immaterial impact on this audit. The reported requirements remain the same.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

ships includes medical, personnel, training, and other administrative records. Therefore, PII should be included as an assessable unit at the ship level to ensure that adequate internal controls are maintained over PII, and to preclude unintentional or unauthorized release.

(2) COMNAVAILANT did not have supporting documentation to validate their claim of reasonable assurance as reported on the annual Statements of Assurance for 10 COMNAVAILANT activities for FY 2013. Commands should have reliable and readily available documentation with an audit trail to support the annual Statement of Assurance. This documentation of internal control activities should be maintained for subsequent review by management, inspector general, and audit personnel. The absence of available supporting documentation implies that management's judgment of reasonable assurance was made without having sufficient and adequate management controls in place.

(3) These conditions occurred primarily due to the need for increased management oversight of ship operations by COMNAVSURFLANT and COMNAVAILANT. The COMNAVSURFLANT Inspector General's office told us that there were no MIC program managers at the ship level to coordinate the annual submission of the Statement of Assurance because of insufficient manpower in their office.

(4) Consequently, it would be inappropriate to conclude that internal controls for PII on COMNAVSURFLANT and COMNAVAILANT ships were in place and operating effectively at all times if there is no evidence to substantiate that staff performed the required reviews. When sufficient internal controls are not maintained over PII, the potential risk of identity theft or fraud is increased. Additionally, when various risk areas (armory, ammunition storage, cash, etc.) that should be designated as assessable units are not subject to periodic review, the vulnerability of ships' personnel and operations is increased.

8. Impact. FFC, COMNAVSURFLANT, and COMNAVAILANT do not have reasonable assurance that PII was protected on the ships selected for audit. Insufficient protection of PII increases the risk of unauthorized information disclosure; identify theft, fraud, waste, abuse, and damage to DON's reputation.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

9. Recommendations and Corrective Actions. Our recommendations, summarized management responses, and our comments on the responses follow. Commander, U.S. Fleet Forces Command responded for themselves and for Commander, Naval Surface Force Atlantic and Commander, Naval Air Force Atlantic. The complete text of the management response is in Enclosure 5.

We recommend that Commander, United States Fleet Forces Command:

Recommendation 1. Establish controls and provide oversight to ensure that leadership biographies on Fleet Forces Command accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.

Management response to Recommendation 1. Concur. The U.S. Fleet Forces Command Webmaster will provide oversight to subordinate Echelon III command Webmasters to ensure they are in compliance with applicable instructions, by requiring quarterly spot checks on their public-facing Web sites. Spot checks will be maintained on file for 3 years. Echelon III Webmasters will be required to push the requirement for quarterly spot checks and report compliance down to Echelon IV and V Webmasters. The U.S. Fleet Forces Command Webmaster will perform periodic spot checks of Echelon III command spot checks during quarter 1 and quarter 3 of each fiscal year. The U.S. Fleet Forces Command Privacy Act Coordinator will ensure Echelon III Privacy Act Coordinators include public Web sites and internal portal sites when conducting semi-annual personally identifiable information (PII) spot checks.

Recommendation 2. Establish controls and provide oversight to ensure that Fleet Forces Command Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.

Management response to Recommendation 2. Concur. The U.S. Fleet Forces Command Public Affairs Officer (PAO) will ensure subordinate command PAOs and collateral duty PAOs (CDPAOs) assuming the duties of the Webmaster, are provided training in the posting of appropriate information to public-facing Web sites and to submit a list of PAOs or CDPAOs acting as Webmasters for their subordinate Echelon IV and V Web sites by the end of quarter 1 for Fiscal Year 2015. The U.S. Fleet Forces Command Webmaster will randomly and periodically spot check Echelon IV and V commands by contacting the assigned Webmaster to ensure a trained PAO or CDPAO is actively assuming the duties as command Webmaster in compliance with Secretary of the Navy Instruction 5720.44C.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Naval Audit Service comment on responses to Recommendations 1 and 2. Actions planned meet the intent of the recommendations, which are considered closed as of the date of the management response, 25 September 2014.

We recommend that Commander, Naval Surface Force Atlantic:

Recommendation 3. Implement a Privacy Act program as required by Secretary of the Navy Instruction 5211.5E. At a minimum, the program must ensure that a formal, up-to-date Privacy Act program instruction is in place at the ship level, and ensure that: management procedures and frameworks are established; management roles and responsibilities are defined; systems of records are identified and managed; site visits are conducted; training is identified and when completed, documented; and organizational and higher-level monitoring and oversight procedures and controls are established.

Recommendation 4. Establish controls and provide oversight at the ship level to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with Secretary of the Navy Message 042232Z of October 2007.

Recommendation 5. Establish controls and perform periodic reviews at the ship level to ensure that the disposal processes on ships are sufficient to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.

Recommendation 6. Establish controls and perform periodic reviews at the ship level to ensure that personally identifiable information training is completed and documented by all ship personnel as required by Department of the Navy Chief Information Officer Message 181905Z of December 2008.

Recommendation 7. Monitor and provide oversight at the ship level to ensure that personally identifiable information is properly safeguarded in accordance with Secretary of the Navy Instruction 5211.5E.

Recommendation 8. Establish controls and perform periodic reviews to ensure that a Privacy Act Statement is included on all locally developed ship forms used to collect personally identifiable information, as required by Secretary of the Navy Instruction 5211.5E.

Management response to Recommendations 3-8. Concur. This [items discussed in Recommendations 3-8] will be accomplished at the ship level via

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

the Commander, Naval Surface Force Atlantic Instruction currently being written with an estimated completion date of 31 October 14.

Recommendation 9. Establish controls and provide oversight to ensure that leadership biographies on the commands' accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.

Management response to Recommendation 9. Concur. Biographies are reviewed annually in July by Commander, Naval Surface Force Atlantic N6 Webmaster. Additionally, all ship Web sites, to include biographies, are routinely reviewed by Commander, Naval Surface Force Atlantic PAO. Review of ship Web sites and biographies have been added to Commander, Naval Surface Force Atlantic's Public Affairs annual Manager's Internal Control Program assessments. We will review biographies and make any corrections required no later than 15 July 2015.

Recommendation 10. Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions as required by Secretary of the Navy Instruction 5720.44C.

Management Response to Recommendation 10. Concur. Quarterly training is provided to collateral duty public affairs personnel assigned to Commander, Naval Surface Force Atlantic tenant commands. Commander, Naval Surface Force Atlantic PAO will coordinate with ship Immediate Superiors in Command and Commander, Carrier Strike Group 4 to ensure public affairs training is documented in appropriate training programs (i.e., Fleet Training Management and Planning System) no later then 31 December 2014.

Recommendation 11. Establish a Managers' Internal Control Program at the ship level to evaluate and report on the effectiveness of internal controls and make corrections, when necessary, as required by Secretary of the Navy Instruction 5200.35F.

Management Response to Recommendation 11. Concur. All Naval Ships utilize internal control processes on their assessable units. This is accomplished utilizing various assessments, inspections and evaluations on a regularly scheduled basis, which are identified in the Surface Force Readiness Manual listed under Inspections, Certifications, Assessments and Verifications and Command Readiness Assist Visit. The major difference between assessments performed utilizing the Surface Force Readiness Manual and Manager's Internal Control Program, is not having a centralized mechanism to collect and review the results of all the assessments together in order to submit an annual statement of assurance. Presently, the statement of assurance for the

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

ships is their ability to get underway and perform their mission. The Managers' Internal Control Program is in place as of 30 September 2014.

Recommendation 12. Include personally identifiable information as an assessable unit in the Managers' Internal Control Program in accordance with Secretary of the Navy Instruction 5200.35F.

Management Response to Recommendation 12. Concur. In Commander, Naval Surface Force Atlantic's Manager's Internal Control Program, PII is and has been identified as an assessable unit. For the ships, assessment of PII is performed by the ship's Immediate Superior in Command utilizing the Command Readiness Assist Visit, which is provided to Commander, Naval Surface Force Atlantic N1 annually by 31 December.

Naval Audit Service comment on responses to Recommendations 3-12. Actions planned meet the intent of the Recommendations 3-10, which are considered open.

Actions taken meet the intent of Recommendation 11, which is closed.

Regarding Recommendation 12, in subsequent communication, management informed us that PII was made an assessable unit as of 13 August 2014. Action taken meets the intent of Recommendation 12, and it is considered closed.

We recommend that Commander, Naval Air Force Atlantic:

Recommendation 13. Improve the Privacy Act program at the ship level as required by Secretary of the Navy Instruction 5211.5E. The program must include site visits, training, organizational and higher-level monitoring and oversight procedures, and maintenance of program documentation.

Management Response to Recommendation 13. Concur. A Privacy Act Spot Check requirement will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual (Commander, Naval Air Force Atlantic Instruction 3500.20D). Chapter 5 is titled "Inspections, Certifications and Assessments Required for Certification as Independent Unit Ready for Tasking."

Commander, Naval Air Forces Atlantic CNAL action: Estimated completion date is 30 February 2015, when the revised Aircraft Carrier Training Readiness Manual CVN-TRAMAN (COMNAVAIRFORINST 3500.200) is promulgated.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Recommendation 14. Establish controls and perform periodic reviews of assessable units to ensure that ships are conducting semiannual spot checks, and that proper documentation of inspections is maintained as required by Secretary of the Navy Message R042232Z of October 2007.

Management response to Recommendation 14. Concur. A process is already in place where semi-annual spot checks are indicated in Privacy Act reports that are completed quarterly and reported through Naval Air Force Atlantic to U.S. Fleet Forces Command in accordance with Secretary of the Navy Instruction 5211.5E. Periodic reviews of ships by Naval Air Force Atlantic Privacy Act/PII coordinator will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual.

Recommendation 15. Establish controls and perform periodic reviews at the ship level to ensure that the disposal processes on ships are sufficient to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.

Management response to Recommendation 15. Concur. Periodic reviews of ships by Naval Air Force Atlantic Privacy Act/PII Coordinator will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual.

Commander, Naval Air Forces Atlantic CNAL action: Estimated completion date is 30 February 2015, when the revised Aircraft Carrier Training Readiness Manual CVN-TRAMAN (COMNAVAIRFORINST 3500.200) is promulgated.

Recommendation 16. Monitor and provide oversight at the ship level to ensure that personally identifiable information is properly safeguarded in accordance with Secretary of the Navy Instruction 5211.5E.

Management response to Recommendation 16. Concur. Periodic reviews of ships by Naval Air Force Atlantic Privacy Act/PII coordinator will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual.

Commander, Naval Air Forces Atlantic CNAL action: Estimated completion date is 30 February 2015, when the revised Aircraft Carrier Training Readiness Manual CVN-TRAMAN (COMNAVAIRFORINST 3500.200) is promulgated.

Recommendation 17. Establish controls and provide oversight to ensure that leadership biographies on the commands' accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Management response to Recommendation 17. Concur. Ship Web sites are maintained in accordance with Secretary of the Navy instructions. Sites are reviewed for discrepancies during the Training Readiness Assist Program conducted by Naval Air Force Atlantic prior to integrated training.

Commander, Naval Air Force Atlantic action: Completed.

Recommendation 18. Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.

Management response to Recommendation 18. Concur. Media Departments receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C, during TRAP, C2X certification from CSG-4, and during weekly departmental training.

Commander, Naval Air Force Atlantic action: Completed.

Recommendation 19. Maintain documentation of internal control activities to ensure effective operations for subsequent review by management, inspector general, and audit personnel in accordance with Secretary of the Navy Instruction 5200.35F.

Management response to Recommendation 19. Concur. The Commander, Naval Air Force Atlantic Inspector General maintains documentation for Commander, Naval Air Force Atlantic Headquarters Manager's Internal Control Program. The Manager's Internal Control Program documentation was provided to the Naval Audit Service audit team. Subordinate Echelon IV and V commands are required to maintain organizational Manager's Internal Control Program documentation. This requirement is promulgated in paragraph 5 of Commander, Naval Air Force Instruction 5200.1C (Manager's Internal Control Program). A copy of this instruction was provided to the Naval Audit Service audit team. A similar paragraph will be added to the Commander, Naval Air Force Atlantic annual Manager's Internal Control Program plan (COMNAVAIRLANTNOTE 5200) to remind subordinate commands of the requirement to maintain Manager's Internal Control documentation.

Commander, Naval Air Force Atlantic action: Estimated completion date is 30 November 2014 when the annual Manager's Internal Control plan is promulgated.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

Naval Audit Service comment on responses to Recommendations 13 through 19. Actions planned meet the intent of the recommendations. In subsequent communication, management indicated that the target completion dates for Recommendations 13-16 is 28 February 2015, and these recommendations are consider open. Recommendation 19 is also considered open.

Recommendations 17 and 18 are considered closed as of the date of the management response on 30 September 2014.

10. Other Information.

a. Actions taken by the Commander, United States Fleet Forces Command; Commander, Naval Surface Force Atlantic; and Commander, Naval Air Force Atlantic meet the intent of Recommendations 1-2, 11-12, and 17-18, and the recommendations are closed. Actions planned by the Commander, United States Fleet Forces Command, Commander, Naval Surface Force Atlantic and Commander, Naval Air Force Atlantic meet the intent of Recommendations 3-10, 13-16, and 19. 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 within 30 days after target completion dates. Please provide all correspondence to the Acting Assistant Auditor General for Financial Management and Comptroller Audits, XXXXXXXX, XXXXXXXXXXXXXXXXXXXX, with a copy to the Director, Policy and Oversight, XXXXXXXX, XXXXXXXXXXXXXXXXXXXX. 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)

b. 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).

c. 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-NAVAUDSVC Web sites, or post in Navy Taskers without the prior approval of the Auditor General of the Navy.

Subj: **MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(AUDIT REPORT N2015-0003)**

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



FOIA (b)(6)

LUTHER N. BRAGG
Acting Auditor General

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)
DON CIO
NAVINGEN (NAVIG-14)
AFAA/DO

Enclosure (1):**Status of Recommendations**

Recommendations							
Finding ³	Rec. No.	Page No.	Subject	Status ⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ⁵
1	1	9	Establish controls and provide oversight to ensure that leadership biographies on Fleet Forces Command accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.	C	Commander, United States Fleet Forces Command	9/25/2014	
1	2	9	Establish controls and provide oversight to ensure that Fleet Forces Command Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.	C	Commander, United States Fleet Forces Command	9/25/2014	
1	3	10	Implement a Privacy Act program as required by Secretary of the Navy Instruction 5211.5E. At a minimum, the program must ensure that a formal, up-to-date Privacy Act program instruction is in place at the ship level, and ensure that: management procedures and frameworks are established; management roles and responsibilities are defined; systems of records are identified and managed; site visits are conducted; training is identified and when completed, documented; and organizational and higher-level monitoring and oversight procedures and controls are established.	O	Commander, Naval Surface Force Atlantic	10/31/2014	
1	4	10	Establish controls and provide oversight at the ship level to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with Secretary of the Navy Message 042232Z of October 2007.	O	Commander, Naval Surface Force Atlantic	10/31/2014	

³ / + = Indicates repeat finding.

⁴ / 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.

⁵ If applicable

Recommendations							
Finding ³	Rec. No.	Page No.	Subject	Status ⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ⁵
1	5	10	Establish controls and perform periodic reviews at the ship level to ensure that the disposal processes on ships are sufficient to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Surface Force Atlantic	10/31/2014	
1	6	10	Establish controls and perform periodic reviews at the ship level to ensure that personally identifiable information training is completed and documented by all ship personnel as required by Department of the Navy Chief Information Officer Message 181905Z of December 2008.	O	Commander, Naval Surface Force Atlantic	10/31/2014	
1	7	10	Monitor and provide oversight at the ship level to ensure that personally identifiable information is properly safeguarded in accordance with Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Surface Force Atlantic	10/31/2014	
1	8	10	Establish controls and perform periodic reviews to ensure that a Privacy Act Statement is included on all locally developed ship forms used to collect personally identifiable information, as required by Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Surface Force Atlantic	10/31/2014	
1	9	11	Establish controls and provide oversight to ensure that leadership biographies on the commands' accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.	O	Commander, Naval Surface Force Atlantic	7/15/2015	
1	10	11	Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions as required by Secretary of the Navy Instruction 5720.44C.	O	Commander, Naval Surface Force Atlantic	12/31/2014	
1	11	11	Establish a Managers' Internal Control Program at the ship level to evaluate and report on the effectiveness of internal controls and make corrections, when necessary, as required by Secretary of the Navy Instruction 5200.35F.	C	Commander, Naval Surface Force Atlantic	9/30/2014	
1	12	12	Include personally identifiable information as an assessable unit in the Managers' Internal Control Program in accordance with Secretary of the Navy Instruction 5200.35F.	C	Commander, Naval Surface Force Atlantic	8/13/2014	

Recommendations							
Finding ³	Rec. No.	Page No.	Subject	Status ⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ⁵
1	13	12	Improve the Privacy Act program at the ship level as required by Secretary of the Navy Instruction 5211.5E. The program must include site visits, training, organizational and higher-level monitoring and oversight procedures, and maintenance of program documentation.	O	Commander, Naval Air Force Atlantic	2/28/2015	
1	14	13	Establish controls and perform periodic reviews of assessable units to ensure that ships are conducting semiannual spot checks, and that proper documentation of inspections is maintained as required by Secretary of the Navy Message R042232Z of October 2007.	O	Commander, Naval Air Force Atlantic	2/28/2015	
1	15	13	Establish controls and perform periodic reviews at the ship level to ensure that the disposal processes on ships are sufficient to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Air Force Atlantic	2/28/2015	
1	16	13	Monitor and provide oversight at the ship level to ensure that personally identifiable information is properly safeguarded in accordance with Secretary of the Navy Instruction 5211.5E.	O	Commander, Naval Air Force Atlantic	2/28/2015	
1	17	13	Establish controls and provide oversight to ensure that leadership biographies on the commands' accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.	C	Commander, Naval Air Force Atlantic	9/30/2014	
1	18	14	Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.	C	Commander, Naval Air Force Atlantic	9/30/2014	
1	19	14	Maintain documentation of internal control activities to ensure effective operations for subsequent review by management, inspector general, and audit personnel in accordance with Secretary of the Navy Instruction 5200.35F.	O	Commander, Naval Air Force Atlantic	11/30/2014	

Pertinent Guidance

Secretary of the Navy Instruction 5211.5E, “Department of the Navy (DON) Privacy Program,” dated 28 December 2005. This instruction defines personally protected information (now referred to as personally identifiable information, or 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. It promulgates policy regarding the collection, retention, disposal, and safeguarding of PII.

- Each DON activity is responsible for implementing and administering a Privacy Act program under this instruction.
- Navy Echelon II and III Commands must designate a Privacy Act Coordinator to conduct staff assistance visits or program evaluations within their command and lower echelon commands to ensure compliance with the Privacy Act and ensure all personnel are trained.
- DON activities are required to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity.
- According to the instruction, best practices state that DON activities shall ensure that PII is not left out in the open or circulated to individuals not having an official need to know.
- Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction.

Secretary of the Navy Instruction 5210.16, “Department of the Navy (DON) Forms Management and Information Requirements (Reports) Management Programs,” dated 31 December 2005. This instruction includes the following DON policy:

- When a DON command requires a form to collect PII, they shall use, in order of precedence, General Services Administration Standard or Optional forms, then Department of Defense forms, and finally, existing DON forms. The last option is to create a new DON form.
 - A new form requires approval and assignment of a form number from the Service Forms Manager.
- Forms that solicit personal information directly from an individual shall include a Privacy Act Statement that apprises the individual of the authority that authorizes collection, the purpose of the collection, who shall routinely have access to the

information, and whether disclosure is voluntary or mandatory. Once filled in, the form shall be marked “FOR OFFICIAL USE ONLY.”

- Forms and information collections that solicit personal information shall be cleared through the Chief of Naval Operations (DNS-36) to ensure that there is an existing Privacy Act System of Records Notice that permits such collection.

Secretary of the Navy Instruction 5200.35E, “DON Managers’ Internal Control (MIC) Program,” dated 8 November 2006.⁶ This is a DON policy that requires commands to establish MIC programs to evaluate and report on the effectiveness of internal controls throughout their organizations and make corrections when necessary. Commands shall use organizational assessments, evaluations, and other contributing information (including performance metrics, external audits, and inspections) as forms of monitoring internal controls. DON organizations shall implement a system of internal controls to provide reasonable assurance that the following objectives are met: (1) effectiveness and efficiency of operation, (2) reliability of financial reporting, and (3) compliance with applicable laws. It defines an assessable unit as any organization, function, program, or subdivision capable of being evaluated by internal control assessment procedures.

Secretary of the Navy Instruction 5720.44C, “DON Public Affairs Policy and Regulations,” dated 21 February 2012. This instruction provides policy and regulations for carrying out DON’s public affairs (PA) and internal relations programs. Each command and activity shall ensure their PA personnel receive periodic training on the performance of PA functions, as well as Internet use. Command and activity Web site biographies cannot be published with date of birth, age, current residential street address, or any information about family members. Place of birth, if desired to be included, will be presented as “... is a native of ...”

- Per Chapter 7, Section 0700, Paragraph 1.c: “While its inherent global accessibility makes the Web a powerful public information tool and enhances productivity in the conduct of daily business, it also presents a potential risk to DON personnel, assets, and operations if inappropriate information is published. Threats to the security of Navy and Marine Corps operations and the safety of DON personnel and their families can come in the form of attacks on computer systems, terrorist attacks on units or personnel, and identity theft. The need to provide public information to the Navy’s and Marine Corps’ various audiences and gain efficiencies by conducting certain business processes via the Internet must be balanced with the need to maintain personal safety, operational and information security, protect personally identifiable information and abide by privacy regulations.”

⁶ Subsequent to audit field work the Secretary of the Navy (SECNAV) Instruction was updated to SECNAV Instruction 5200.35F, dated 21 July 2014. An analysis of the wording shows changes with immaterial impact on this audit. The reported requirements remain the same.

Secretary of the Navy Message R042232Z, “DON PII Annual Training Policy,” dated October 2007. This message requires safeguarding PII across the Department by establishing annual awareness training requirements and semi-annual spot checks. Specifically, commanders/commanding officers/officers-in-charge will ensure that supervisors conduct a spot check of their assigned areas of responsibility, focusing on those areas that deal with PII on a regular basis. This action was to be initially completed by 1 January 2008 and performed semi-annually thereafter. The message also requires that auditable records be maintained by the command’s Privacy Act Coordinator or designated official.

DON Chief Information Officer Naval Message 201839Z, “PII on DON Shared Drives and Application Based Portals,” dated November 2008. This document reinforces current DON policy aimed at reducing the number and potential impact of lost, stolen, or compromised PII to Sailors, Marines, Government personnel, dependents, and DON contractors. It requires that command leadership must ensure proper controls and permissions are in place to safeguard PII found on shared drives and portals. Only those personnel with a need to know should have access to these privacy-sensitive files.

DON Chief Information Officer Naval Message 032009Z, “DON Policy Updates for Personal Electronic Devices (PED) Security and Application of Email Signature and Encryption,” dated October 2008. This message provides updates to the DON policy regarding digital signatures and encryption of e-mail. DON users shall digitally sign e-mail messages requiring either message integrity and/or non-repudiation, and encrypt messages containing sensitive information. E-mail encryption is being used more often as a means to protect e-mail containing PII, Privacy Act information, and other categories of DoD-sensitive information while in transit across the global information grid.

Enclosure (3):

Scope and Methodology

We conducted this audit of managing personally identifiable information (PII) on selected Commander, U.S. Fleet Forces Command (FFC) ships from 14 August 2013 to 26 August 2014. The audit covered selected ships of Commander, Naval Surface Force Atlantic (COMNAVSURFLANT) and Commander, Naval Air Force Atlantic (COMNAVAIRLANT). We judgmentally selected five ships based on their availability at their homeports of Norfolk and Little Creek, VA. We reviewed a total of 38 departments on the 5 selected ships. Enclosure 4 includes a list of activities and ships visited.

We reviewed internal controls by looking at policies and procedures related to PII. We reviewed matters related to the Privacy Act program: Privacy Act Statements; semi-annual spot checks; training and safeguarding PII; records retention and disposal; and PII breach reporting. We examined Fiscal Years (FYs) 2012 and 2013 Managers' Internal Control Program reports to see if PII was identified as an assessable unit and if any deficiencies were noted and corrected.

We also evaluated procedures, monitoring practices, and safeguarding measures by conducting physical inspections to verify proper safeguarding and disposal of PII. To test the safeguarding of PII on computers, we judgmentally selected computers for review from the five ships.⁷ In each department with computer(s) on each ship, we selected at least one or more computers for examination. We analyzed training records for FY 2013. We looked at COMNAVSURFLANT and COMNAVAIRLANT ship-generated forms used to collect PII to determine whether they included a Privacy Act Statement. We also reviewed the publically accessible official navy.mil Web pages and the officially registered social media sites of FFC, COMNAVSURFLANT, COMNAVAIRLANT, and the five selected ships to ensure that posted information that was within the control of the command personnel did not contain PII.

We interviewed Managers' Internal Control Program Coordinators, Privacy Act coordinators and managers, and personnel responsible for implementing the Privacy Act program at FFC, COMNAVSURFLANT, and COMNAVAIRLANT, and on the selected ships. We also interviewed the personnel responsible for the homepage Web sites of FFC, COMNAVSURFLANT, COMNAVAIRLANT, and the selected ships.

We assessed compliance with applicable laws and regulations, including Department of Defense (DoD) and Department of the Navy regulations applicable to PII. We also reviewed prior Naval Audit Service, DoD Inspector General, and Government

⁷ We did not determine the total number of computers at the five U.S. Fleet Forces ships.

Accountability Office audit reports. There were no previous audit reports directly covering management of PII on FFC ships on which to follow up.

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.

Enclosure (4):

Activities Visited

Commander, United States Fleet Forces Command, Norfolk, VA

Commander, Naval Surface Force Atlantic, Norfolk, VA

USS NORMANDY, Norfolk, VA

USS NITZE, Norfolk, VA

USS GONZALEZ, Norfolk, VA

USS GUNSTON HALL, Little Creek, VA

Commander, Naval Air Force Atlantic, Norfolk, VA

USS GEORGE H.W. BUSH, Norfolk, VA

Enclosure (5):

Management Response from Commander, U.S. Fleet Forces Command



DEPARTMENT OF THE NAVY
COMMANDER
U.S. FLEET FORCES COMMAND
1982 WITSCHER AVENUE SUITE 250
NORFOLK, VA 23551-2497

7510
Ser N01P/
25 Sep 14

From: Commander, U.S. Fleet Forces Command (N01P)
To: Commander, U.S. Fleet Forces Command (N01IG)

Subj: RESPONSE TO NAVAL AUDIT SERVICE DRAFT AUDIT REPORT
MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON
SELECTED COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
N2013-025)

Ref: (a) NAVAUDSVC Memo 7510 N2013-025 dated 24 Jul 13
(b) SECNAVINST 7510.7P, "Department of the Navy
Internal Audit"

Encl: (1) Response to Naval Audit Service Draft Audit Report
Invoice Management on Selected Ships of Commander,
U.S. Fleet Forces Command, (2013-013)

1. In response to findings and recommendations under reference (a), enclosure (1) is provided.
2. Response submitted per reference (b).



FOIA (b)(6)

Copy to:
N01P1 (BAC)
N02IG

Enclosure (5)
Page 1 of 2

RESPONSE TO NAVAL AUDIT SERVICE DRAFT AUDIT REPORT MANAGING
PERSONALLY IDENTIFIABLE INFORMATION ON SELECTED COMMANDER, U.S.
FLEET FORCES COMMAND SHIPS (N2013-025)

Recommendation 1

Establish controls and provide oversight to ensure leadership biographies on commands' accessible web pages are compliant with Secretary of the Navy Instruction 5620.44C.

Response: USFF concurs with this recommendation. USFF Webmaster will provide oversight to subordinate Echelon III command webmasters to ensure they are in compliance with applicable instructions, by requiring quarterly spot checks on their public-facing websites. Spot checks will be maintained on file for three years. Echelon III webmasters will be required to push the requirement for quarterly spot checks and report compliance down to Echelon IV and V webmasters. USFF Webmaster will perform periodic spot checks of Echelon III command websites, and semi-annual review of Echelon III command spot checks during quarter 1 (Q1) and quarter 3 (Q3) of each fiscal year (FY). USFF Privacy Act Coordinator will ensure Echelon III Privacy Act Coordinators include public websites and internal portal sites when conducting semi-annual PII spot checks.

Recommendation 2

Establish controls and provide oversight to ensure Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.

Response: USFF concurs with this recommendation. USFF Public Affairs Officer will ensure subordinate command PAOs and collateral duty PAOs (CDPAO) assuming the duties of webmaster, are provided training in the posting of appropriate information to public-facing web sites and to submit a list of PAOs or CDPAOs acting as webmasters for their subordinate Echelon IV and V web sites by the end of quarter 1 (Q1) for FY 15. The USFF Webmaster will randomly and periodically spot check Echelon IV and V commands by contacting the assigned webmaster to ensure a trained PAO or CDPAO is actively assuming the duties as command webmaster in compliance with SECNAVINST 5720.44C.

Enclosure (1)

Enclosure (6):

Management Response from Commander, Naval Surface Force Atlantic



DEPARTMENT OF THE NAVY
COMMANDER
NAVAL SURFACE FORCE ATLANTIC
BOX 16E, 1751 MORRIS STREET
NORFOLK, VIRGINIA 23511-2808

7510
Ser N01IG/979
16 Oct 14

From: Commander, Naval Surface Force Atlantic
To: Navy Audit Service, Audit Director for Managing
Personally Identifiable Information on Selected Commander,
U.S. Fleet Forces Command Ships

Subj: MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON SELECTED
COMMANDER, U.S. FLEET FORCES COMMAND SHIPS
(DISCUSSION DRAFT 2013-025)

Ref: (a) Email from [REDACTED] USFF, N01G, of 2 Sep 14
(b) NAVAUDSVC Draft Audit Report 7510 2013-025, dated
26 Aug 14

Encl: (1) Commander, Naval Surface Force Atlantic response to
subject discussion draft (2013-025)

1. Per references (a) and (b), the subject draft discussion is
forwarded for review and comments. Additionally, enclosure (1)
contains our response.

2. Please refer any questions to [REDACTED]
COMNAVSURFLANT IG, at [REDACTED]

[REDACTED]

Chief of Staff

FOIA (b)(6)

FOIA (b)(6)

FOIA (b)(6)

~~FOR OFFICIAL USE ONLY~~ – DISCUSSION DRAFT RESPONSE

MANAGING PERSONALLY IDENTIFIABLE INFORMATION ON SELECTED
COMMANDER, U.S. FLEET FORCES COMMAND SHIPS (DISCUSSION
DRAFT 2013-025)

Recommendation 3: Implement a Privacy Act program as required by Secretary of the Navy Instruction 5211.5E. At a minimum, the program must ensure that a formal, up-to-date Privacy Act program instruction is in place at the ship level, and ensure that: management procedures and frameworks are established; management roles and responsibilities are defined; systems of records are identified and managed; site visits are conducted; training is identified and when completed, documented; and organizational and higher-level monitoring and oversight procedures and controls are established.

CNSL Response: Concur. This will be accomplished through a COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 4: Establish controls and provide oversight at the ship level to ensure that semiannual personally identifiable information spot checks are conducted and documented, and that all spot check areas are reviewed semiannually in accordance with Secretary of the Navy Message 042232Z of October 2007.

CNSL Response: Concur. This will be accomplished at the ship level via the COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 5: Establish controls and perform periodic reviews at the ship level to ensure that the disposal processes on ships are sufficient to render personally identifiable information records unrecognizable or beyond reconstruction as required by Secretary of the Navy Instruction 5211.5E.

CNSL Response: Concur. This will be accomplished at the ship level via the COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 6: Establish controls and perform periodic reviews at the ship level to ensure that personally identifiable information training is completed and documented by all ship personnel as required by Department of the Navy Chief Information Officer Message 181905Z of December 2008.

We have determined that this page of the management response does not include information that should be marked FOR OFFICIAL USE ONLY; therefore, we are striking through the FOUO marking on this letter.

CNSL Response: Concur. This will be accomplished at the ship level via the COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 7: Monitor and provide oversight at the ship level to ensure that personally identifiable information is properly safeguarded in accordance with Secretary of the Navy Instruction 5211.5E.

CNSL Response: Concur. This will be accomplished at the ship level via the COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 8: Establish controls and perform periodic reviews to ensure that a Privacy Act Statement is included on all locally developed ship forms used to collect personally identifiable information, as required by Secretary of the Navy Instruction 5211.5E.

CNSL Response: Concur. This will be accomplished at the ship level via the COMNAVSURFLANT Instruction currently being written with an estimated completion date of 31 Oct 14.

Recommendation 9: Establish controls and provide oversight to ensure that leadership biographies on the commands' accessible Web pages are compliant with Secretary of the Navy Instruction 5720.44C.

CNSL Response: Concur. Biographies are reviewed annually in July by CNSL N6 Webmaster. Additionally, all ship websites, to include biographies, are routinely reviewed by CNSL PAO. Review of ship websites and biographies have been added to CNSL's Public Affairs annual MICP assessments. We will review biographies and make any corrections required no later than 15 July 2015.

Recommendation 10: Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions as required by Secretary of the Navy Instruction 5720.44C.

CNSL Response: Concur. Quarterly training is provided to collateral duty public affairs personnel assigned to CNSL tenant commands. CNSL PAO will coordinate with ship ISICs and Commander, Carrier Strike Group 4 to ensure public affairs training is documented in appropriate training programs (i.e. FLTMPs) no later the 31 Dec 2014.

Recommendation 11: Establish a Managers' Internal Control Program at the ship level to evaluate and report on the effectiveness of internal controls and make corrections, when necessary, as required by Secretary of the Navy Instruction 5200.35F.

CNSL Response: Concur. All Naval Ships utilize internal control processes on their assessable units. This is accomplished utilizing various assessments, inspections and evaluations on a regularly scheduled basis which are identified in the Surface Force Readiness Manual (SFRM) listed under Inspections, Certifications, Assessments and Verifications (ICAV) and Command Readiness Assist Visit (CRAV).

The major difference between assessments performed utilizing the SFRM and MICP, is not having a centralized mechanism to collect and review the results of all the assessments together in order to submit an annual statement of assurance. Presently, the statement of assurance for the ships is their ability to get underway and perform their mission. The Managers' Internal Control Program is in place as of 30 Sep 2014.

Recommendation 12: Include personally identifiable information as an assessable unit in the Managers' Internal Control Program in accordance with Secretary of the Navy Instruction 5200.35F.

CNSL Response: Concur. In CNSL's MICP, PII is and has been identified as an assessable unit. For the ships, assessment of PII is performed by the ship's Immediate Superior In Command (ISIC) utilizing the CRAV which is provided to CNSL's N1 annually by 31 Dec.

Enclosure (7):

Management Response from Commander, Naval Air Force Atlantic



DEPARTMENT OF THE NAVY
COMMANDER NAVAL AIR FORCE ATLANTIC
1279 FRANKLIN ST.
NORFOLK, VIRGINIA 23511-2494

7510
Ser N01/625
30 Sep 14

From: Commander, Naval Air Force Atlantic
To: Naval Audit Service

Subj: DRAFT AUDIT REPORT - MANAGING PERSONALLY IDENTIFIABLE
INFORMATION ON SELECTED COMMANDER, U.S. FLEET FORCES
COMMAND SHIPS (2013-025)

Ref: (a) NAVAUDSVC Draft Audit Report of 26 August 2014

Encl: (1) COMNAVAIRLANT responses to subject draft report

1. Per reference (a), enclosure (1) is forwarded in response to
the draft report recommendations.

2. The point of contact is [REDACTED] COMNAVAIRLANT
Inspector General, [REDACTED] e-mail: [REDACTED].

[REDACTED]
[REDACTED]
Chief of Staff

Copy to:
COMNAVAIRLANT (N001G, N01L, N01P, N7)

FOIA (b)(6)

FOIA (b)(6)

Enclosure (7)
Page 1 of 4

Recommendation 13: Improve the Privacy Act program at the ship level as required by Secretary of the Navy Instruction 5211.5E. The program must include site visits, training, organizational and higher-level monitoring and oversight procedures, and maintenance of program documentation.

CNAL Response: (Privacy Act/PII Coordinator)

Concur. A Privacy Act Spot Check requirement will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual (CVN-TRAMAN), COMNAVAIRLANTINST 3500.20D. Chapter 5 is titled "Inspections, Certifications and Assessments Required for Certification as Independent Unit Ready for Tasking.

CNAL Action: Estimated completion date is 30 February 2015 when the revised CVN-TRAMAN (COMNAVAIRFORINST 3500.20D) is promulgated.

Recommendation 14: Establish controls and perform periodic reviews of assessable units to ensure that ships are conducting semiannual spot checks, and that proper documentation of inspections is maintained as required by Secretary of the Navy Message R042232Z of October 2007.

CNAL Response: (Privacy Act/PII Coordinator)

Concur. A process is already in place where semi-annual spot checks are indicated in Privacy Act reports that are completed quarterly and reported through AIRLANT to U.S. Fleet Forces Command in accordance with SECNAVINST 5211.5E. Periodic reviews of ships by AIRLANT Privacy Act/PII coordinator will be added to Chapter 5 of the CVN-TRAMAN.

CNAL Action: Estimated completion date is 30 February 2015 when the revised CVN-TRAMAN (COMNAVAIRFORINST 3500.20D) is promulgated.

Recommendation 13: Improve the Privacy Act program at the ship level as required by Secretary of the Navy Instruction 5211.5E. The program must include site visits, training, organizational and higher-level monitoring and oversight procedures, and maintenance of program documentation.

CNAL Response: (Privacy Act/PII Coordinator)

Concur. A Privacy Act Spot Check requirement will be added to Chapter 5 of the Aircraft Carrier Training Readiness Manual (CVN-TRAMAN), COMNAVAIRLANTINST 3500.20D. Chapter 5 is titled "Inspections, Certifications and Assessments Required for Certification as Independent Unit Ready for Tasking.

CNAL Action: Estimated completion date is 30 February 2015 when the revised CVN-TRAMAN (COMNAVAIRFORINST 3500.20D) is promulgated.

Recommendation 14: Establish controls and perform periodic reviews of assessable units to ensure that ships are conducting semiannual spot checks, and that proper documentation of inspections is maintained as required by Secretary of the Navy Message R042232Z of October 2007.

CNAL Response: (Privacy Act/PII Coordinator)

Concur. A process is already in place where semi-annual spot checks are indicated in Privacy Act reports that are completed quarterly and reported through AIRLANT to U.S. Fleet Forces Command in accordance with SECNAVINST 5211.5E. Periodic reviews of ships by AIRLANT Privacy Act/PII coordinator will be added to Chapter 5 of the CVN-TRAMAN.

CNAL Action: Estimated completion date is 30 February 2015 when the revised CVN-TRAMAN (COMNAVAIRFORINST 3500.20D) is promulgated.

Recommendation 18: Establish controls and provide oversight to ensure that Public Affairs personnel receive periodic training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C.

CNAL Response: (N01P)

Concur. Media Departments receive period training in the performance of public affairs functions, as required by Secretary of the Navy Instruction 5720.44C, during TRAP, C2X certification from CSG-4, and during weekly departmental training.

CNAL Action: Completed.

Recommendation 19: Maintain documentation of internal control activities to ensure effective operations for subsequent review by management, inspector general, and audit personnel in accordance with Secretary of the Navy Instruction 5200.35F.

CNAL Response: (N00IG)

Concur. The CNAL IG maintains documentation for CNAL HQ MIC program. The MIC documentation was provided to the NAVAUDSVC audit team. Subordinate Echelon IV and V commands are required to maintain organizational MIC program documentation. This requirement is promulgated in paragraph 5 of COMNAVAIRFOR Instruction 5200.1C (Manager's Internal Control Program). A copy of this instruction was provided to the NAVAUDSVC audit team. A similar paragraph will be added to the CNAL annual MIC program plan (COMNAVAIRLANTNOTE 5200) to remind subordinate commands of the requirement to maintain MIC documentation.

CNAL Action: Estimated completion date is 30 November 2014 when the annual MIC plan is promulgated.

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~