



DEPARTMENT OF THE NAVY

NAVAL SERVICE TRAINING COMMAND
2601A PAUL JONES STREET
GREAT LAKES, ILLINOIS 60088-2845

NSTCINST 5211.1
OGC
4 Mar 11

NSTC INSTRUCTION 5211.1

From: Commander, Naval Service Training Command

Subj: NAVAL SERVICE TRAINING COMMAND PRIVACY PROGRAM

Ref: (a) SECNAVINST 5211.5E
(b) DON CIO WASHINGTON DC 171952Z Apr 07
(c) SECNAVINST 5210.8D
(d) DON CIO WASHINGTON DC 291652Z Feb 08
(e) SECNAV M-5210.1
(f) NETCINST 5211.2
(g) 5 USC 552a

Encl: (1) [NSTC Systems of Records](#)
(2) [PII Spot Check Form](#)
(3) [Best Practices Protocol for Printed and Electronic Media](#)
(4) [Employee/Supervisor Certification of Initial/Annual Refresher Training](#)

1. Purpose. The purpose of this instruction is to implement Privacy Act (PA) actions and policies required by references (a) through (g) for the commands, activities, and personnel of the Naval Service Training Command (hereinafter NSTC or the Command).

2. Cancellation. NSTCNOTE 5211.

3. Background. The Privacy Act of 1974 (reference (g)), promulgated within the DON by reference (a), requires Federal Government agencies to protect the privacy of individuals whose records they maintain and to grant such individuals the right to access and correct such records.

4. Definitions. Unless otherwise stated in this instruction, all defined terms (denoted by an initial capital letter) shall have the same meaning as those in paragraph 4 of reference (a) and paragraphs 4 and 5 of reference (d).

5. Action:

a. Office of General Counsel (OGC):

(1) Is hereby designated as the Command Privacy Act Coordinator (PAC) to perform the duties in paragraph 7(h) of reference (a) for all NSTC commands and activities. As such, OGC is the principal point of contact for all PA matters, including but not limited to reporting Personally Identifiable Information (PII) breaches and acting as the point of contact (POC) for all follow-up actions and individual notifications regarding any breach. Commands and activities subordinate to NSTC must contact OGC in the event of any actual or suspected breach and shall act only through NSTC OGC.

(2) Provides assistance when notified by a command, activity, department, or PA System Administrator of the need to establish a new System of Records, amend or alter or delete an existing System of Records. Notifies and coordinates all such changes with CNO (DNS-36). Current Systems of Records used by NSTC are listed at enclosure (1).

(3) Semi-annually (April and October) coordinates a review of NSTC PA practices Command-wide to determine compliance with all requirements and to ensure that basic PII safeguards are in place. This review will be conducted using the PII Spot Check Form attached as enclosure (2). The review shall include, but not be limited to:

(a) Evaluation of the continued need for, and efficacy of, all internal directives, forms, practices, and procedures that have PA implications, especially those which contain a Privacy Act Statement or solicit PII;

(b) Compliance with all PA training requirements;

(c) Identification in writing to the NSTC PAC of all currently appointed PA Office Administrators (previously designated as PA POC's) and any System of Records Administrators.

b. NSTC Command Logistics and Information Officer (N4/6):

(1) Provides guidance for effective assessment and utilization of privacy-related technologies.

(2) Develops and coordinates privacy policy, procedures, education, training, and awareness practices regarding NSTC information systems.

(3) Enforces the policy set forth in reference (b) prohibiting any PII on NSTC portable storage devices. Approves or disapproves exceptions to this policy in writing on a case by case basis.

(4) Provides guidance to System of Records Administrators on the conduct of Privacy Impact Assessments (PIAs) of NSTC information systems. Oversees NSTC PIA policy and procedures to ensure PIAs are conducted commensurate with the information system being assessed, the sensitivity of PII in that system, and the risk of harm for unauthorized release of that information.

(5) Reviews all NSTC PIAs prior to requesting approval by chain of command (NETC N6 or N16/MPTE CIO) as required.

(6) Ensures NSTC compliance with DoN World Wide Web and information systems privacy requirements, including use of encryption software and implementation of prescribed privacy-related technologies.

(7) Provides input as required for inclusion in the Federal Information Systems Management Act (FISMA) Report.

c. Commanding Officers, Directors, Department Heads and Special Assistants shall each:

(1) Within one half hour of discovery of a loss or suspected loss of PII, directly notify the NSTC PAC (at all times, including after duty hours) by forwarding an e-mail explaining the information listed below:

(a) The date of the incident, number of individuals impacted, and whether they are government civilian, military, and/or private citizens (include percentage of each category); and

(b) A brief description of the incident, including circumstances of the breach, type of information lost or compromised, and if the PII was encrypted or password protected.

(2) Implement written PA guidance, to the extent that additional guidance is deemed necessary.

(3) Appoint a PA Office Administrator in writing that clearly defines the PA Office Administrator's roles and responsibilities. If the command, department, or office maintains one of the Systems of Records noted in enclosure (1), also appoint a System of Records Administrator. Notify the NSTC PAC of the name and contact information of these appointees.

(4) Ensure that information maintained about individuals is complete, relevant, timely, necessary, and required to accomplish a purpose of the activity. Under no circumstances shall PII be collected and retained if no Navy System of Records notice permits collection of such information. Current Navy Systems of Records can be found at the Navy's privacy website, <http://www.privacy.navy.mil>.

(5) Work closely with, and ensure that, the PA System of Records Administrators are properly trained on their duties and responsibilities for protecting PII or other PA protected information in the System of Records they maintain. Ensure that only those DoD/DON officials with a "need to know" in the official performance of their duties have access to information contained in a System of Records.

(6) Ensure consistency with the Federal Acquisition Regulation (FAR):

(a) Ensure that contracts which require a contractor to maintain or operate a System of Records clearly identify each such System of Records;

(b) Incorporate into the solicitation and resulting contract the terms and conditions prescribed by the FAR for the protection of PA protected information, including the proper means of disposing of any PII at the end of the contract term or earlier termination of the contract; and

(c) Ensure contractors are informed of their responsibilities regarding information protected by the PA, particularly the need to comply with all protocols and best practices for handling PII.

(7) Work closely with the NSTC Public Affairs Officer and N6 Information Assurance Manager to prevent PII from being placed on public web sites or in on-line public folders.

(8) Ensure personnel (managers, employees and contractors) who deal with PA receive initial PA training within 30 days of employment with the Command and annual refresher training thereafter. Maintain for two years after the date of training a copy of the Certification of Initial/Annual Refresher Training Certificate (enclosure 4) for each person who has successfully completed the initial and annual training and other program reviews. These certificates will be reviewed during spot checks.

(9) Ensure portable storage devices do not contain any PII unless a written waiver permitting such use has first been obtained from the NSTC Command Logistics and Information Officer (N4/6).

(10) Semi-annually (April and October) conduct and complete reviews of PA Systems of Records to ensure that they are necessary, accurate, and complete and ensure compliance with all PA training requirements. Use the PII Spot Check Form attached as enclosure (2) to conduct this review.

(11) Maintain liaison with records management officials concerning records maintenance and disposal procedures and standards, as appropriate.

(12) Follow the best practices set forth in enclosure (3). These practices are intended to be a starting point and are not to be regarded as an exhaustive list of all possible best practices.

d. System Administrators shall:

(1) Establish appropriate administrative, technical, and physical safeguards to ensure the records in the Systems of Records they maintain or use are protected from unauthorized alteration, destruction, or disclosure.

(2) Protect records from reasonably anticipated threats or hazards and from any disclosures that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(3) Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PII contained in each System of Records used.

(4) Ensure that records are kept in accordance with retention and disposal requirements set forth in reference (e), and are maintained in accordance with the identified PA Systems of Records notice.

(5) Advise the PAC promptly of the need to establish a new System of Records or amend, alter, or delete an existing System of Records.

(6) Semi-annually (April and October) review internal directives, forms, practices, and procedures, including those having PA implications, especially those where a Privacy Act Statement is used or PII are solicited to ensure that they are necessary, accurate, and complete. Report findings to the PAC in writing.

e. Command Assessment/Inspector General: Conduct staff assistance visits or program evaluations within NSTC and lower echelon commands to ensure compliance with the PA.

f. All NSTC Personnel shall:

(1) Ensure portable storage devices comply with all directives concerning PII, including actions intended to safeguard such information.

(2) Ensure that PII contained in a System of Records is protected so that the security and confidentiality of the information is preserved.

(3) Not disclose any information contained in a System of Records by any means to any person or agency, except as authorized by reference (a), or the specific PA Systems of Records notice. All requests for disclosure to anyone outside DoD must be reviewed and cleared by the PAC before any release.

(4) Not maintain unpublished official files that fall under the provisions of the PA.

(5) Safeguard the privacy of individuals and confidentiality of PII.

(6) In those instances where transmittal of PII is necessary, take every step to properly mark correspondence so the recipient is aware of the need to properly protect the information. Double wrap mail containing PII. Address the internal wrapper to the intended recipient and mark it "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES." Electronic transmissions shall be encrypted and password protected.

(7) Not maintain privacy sensitive information in public folders, whether in hard copy or on line.

(8) Immediately report any unauthorized disclosure of PII to the PAC.

(9) Immediately report maintenance of any unauthorized System of Records to the PAC.

(10) To protect against inadvertent disclosure of dated information, dispose of records in a System of Records in accordance with all applicable guidance, including the System of Records notice and reference (e). Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Paper documents should be shredded using a cross-cut shredder whenever possible. Magnetic media is considered cleared and can be disposed of, recycled, or reused only if it has been degaussed a minimum of two times and there is absolute assurance that PII is not and will not thereby be compromised. Failure to render records unrecognizable and unretrievable prior to submitting them for recycling or reuse may constitute an unauthorized release under reference (a).

6. Processing Privacy Act Records. Records protected by the Privacy Act and requested for release within DoD shall be released only to those with a need to know. All requests for release of records to anyone outside DoD shall be referred to the PAC for a release determination. Under no circumstances will any records be released to anyone outside DoD prior to such a determination.

4 Mar 11

7. Privacy Act Team. A Command Privacy Act Team (PA Team) consisting of the Chief of Staff, the PAC, the NSTC Inspector General, the Administrative Officer, the Public Affairs Officer or representative, and the Command Information Officer (CIO) shall meet at 1300 on the first Thursday of each calendar quarter, or more frequently if needed. The Privacy Act Team will:

a. Identify ways to restrict inadvertent releases and unauthorized disclosures of PII and establish best PA practices for NSTC.

b. Each February, review self assessment reports for NSTC and NSTC commands, and activities. Following this review, recommend modifications or revisions to documents and procedures, as appropriate.



DAVID F. STEINDL

Distribution: (NSTCINST 5216.1B)

List 4

Systems of Records used by NSTC

CIG-16	DoD Hotline Program Case Files
CIG-19	Recall Roster/Locator Records
CIG-21	Congressional Correspondence Tracking System
DPR34	Defense Civilian Personnel Data System (DCPDS)
K890.04	Military Personnel Management/Assignment Files
MMN00019	Drug/Alcohol Abuse Report Program
N01070-3	Navy Military Personnel Records System
N01080-1	Enlisted Master File Automated System
N01080-2	Officer Master File Automated System
N01131-1	Officer Selection and Appointment System
N01306-1	Job Advertisement and Selection System (JASS)
NM01500-2	Department of Navy Education and Training Records
N01533-1	Navy Junior ROTC (NJROTC) Applicant/Instructor System
N01533-2	Navy Junior ROTC (NJROTC) Payment Reimbursement System
N05354-1	Equal Opportunity Management Information System
N05041-1	Inspector General (IG) Records
N05100-3	Safety Equipment Needs, Issues, Authorizations
N05520-5	Personnel Security Program Management Records System
N05800-1	Legal Office Litigation/Correspondence Files
N05810-2	Military Justice Correspondence and Information File
N05813-6	Summary and Non-BCD Special Courts Martial Records of Trial
N05819-4	Complaints of Wrong Under Articles 138/1150
N05830-1	JAG Manual Investigative Records
N06110-1	Physical Readiness Information Management System (PRIMS)
N06150-2	Health Care Record System
N07220-1	Navy Standard Integrated Personnel System (NSIPS)
NM07421-1	Time and Attendance Feeder Records
N12290-1	Personnel Action Reporting System
NM126360-1	DoN Voluntary Leave Transfer Program Records
NM12713-1	Equal Employment Opportunity (EEO) Complaint Tracking System
NM12771-1	Discrimination Complaints
NM1500-9	Integrated Learning Environment (ILE) Classes
NM01500-10	Navy Training Management and Planning System (NTMPS)
NM01650-1	Department of the Navy Military Awards System
NM05000-1	General Correspondence Files
NM05000-2	Program Management and Locator System

NM05100-4	WESS Occupational Injuries/Illnesses Log
NM05211-1	Privacy Act Request Files and Tracking System
NM05512-2	Badge and Access Control System
NM05380-1	Combined Federal Campaign/Navy Relief Society
NM05720-1	FOIA Request Appeal Files and Tracking System
NM07320-1	Property Accountability Records
NM12610-1	Hours of Duty Records
NM12630-1	DoN Voluntary Leave Transfer Program Records
T7334	Defense Travel System
T7335	Defense Civilian Pay System

PII Spot Check Form**Date:** _____

This form is an internal document and is to be used by activities leadership to assess the level of compliance in the handling of Personally Identifiable Information (PII) as delineated by law and or specific DoD/DON policy guidance. Where deficiencies are noted, the activity should take immediate corrective action. For additional guidance and information go to the DON Privacy website at www.privacy.navy.mil or contact the NSTC PAC at (847)688-4422/5614 or DSN 792-4422/5614. This Spot Check Form is an auditable record and should be kept on file for two (2) years after it is compiled.

Administrative

1. The name of your PA Office Administrator is _____.

2. The name of the individual assigned to conduct this spot check is _____.

3. The command PA Office Administrator has been identified in writing with clear roles and responsibilities identified.

- a. Yes
- b. No

4. Has the activity implemented Privacy Act guidance additional to that issued in NSTC INSTRUCTION 5211.1, NSTC Privacy Act Program or does the activity believe additional guidance is necessary? If so, please explain.

- a. Yes
- b. No

EXPLAIN:

5. When a loss of PII occurs, the chain of command has a clear understanding of the DON and NSTC reporting policy.

- a. Yes
- b. No

6. How many PII incidents were reported to the NSTC PAC in the past 12 months?

7. Has the activity disseminated guidance to its personnel on how to properly mark email, messages, letters, etc. that contain PII prior to transmission?

- a. Yes
- b. No

8. Has the activity taken action to eliminate or reduce the need for the use of SSNs (including any portion thereof)?

- a. Yes
- b. No
- c. If yes, list actions taken
List: _____

Paper Records

9. At random, spot check 10% of burn bags/locked bins within your activity to ensure that, if they contain PII, they are secure from unauthorized access by individuals who do not have a need to know.

Number of bags checked _____
Number of bags containing PII and not secured _____

10. If the activity does not shred all documents containing PII before they are placed in a recycle container, spot check at random 10% of recycle containers within your activity to ensure that they contain no PII.

Number of containers checked _____
Number of containers containing PII _____

11. Do all forms that collect PII contain a Privacy Act Statement?

- a. Yes
- b. No

12. Does the activity ensure that paper records are not retained indefinitely?

- a. Yes
- b. No

13. Check for the presence of PII on all static or electronic bulletin boards that disseminate information. PII should only be available to individuals with a need to know.

Number of boards checked _____

Number of times where PII was found _____

Number of times where PII should not have been present _____

Electronic Records/Hardware

14. Written procedures IAW reference (b) for all laptops and portable electronic equipment have been created and implemented for all such devices that are transported outside a secure government space. The procedures include a check-in/check-out procedure requiring a supervisory-level signature authorizing removal.

a. Yes

b. No

Number of units not in compliance _____

Not applicable, command has no PDA's _____

15. At random, spot check five (5) laptops and five (5) external hard drives and check no fewer than ten (10) Word Documents for encryption of PII information.

Number of files containing PII _____

Number of files not encrypted _____

16. Does the activity ensure all files on hard drives are routinely reviewed and whenever possible, purged of unnecessary PII?

a. Yes

b. No

17. For activities using shared drives, search and spot check 25% of files that are likely to contain PII (e.g., personnel, medical, safety).

Number of files checked _____

Number of files containing PII _____

18. For DoD IT Portfolio Registry (DITPR) DON registered systems that contain PII for DON personnel and the public, has there been a PIA submitted to the DON CIO office for approval?

Number of systems requiring PIA's _____

Number of systems with PIA's submitted _____

Websites

19. Does the activity have protocols established to ensure PII is not inadvertently posted on a public or restricted access website?

a. Yes

b. No

20. Are activity sponsored websites properly registered?

Number of sites _____

Number properly registered _____

21. Spot check 25% of command web sites to see whether PII is made available to those who do not have a need to know.

Number of sites checked _____

Number of records with PII _____

Training

22. Are there certificates on file indicating that all hands, including contractors, have completed all required PA training for the past two years?

a. Yes

b. No

NSTCINST 5211.1

OGC

4 Mar 11

This page intentionally left blank

Best Practices Protocol for Printed and Electronic Media

1. Review processes and address protections that are in place to ensure that PII is not compromised.
2. Keep all printed copies of data with PII in properly marked folders.
3. Electronic records and transmissions of PII must be properly marked, stored, and disposed. See Paragraph 5 of the NSTC Instruction for guidance.
4. Be certain that PII is not left unprotected and visible on desk tops, file cabinets, photocopy machines, or circulated to individuals who do not have an official need to know.
5. Review web sites (Internet and Intranet) to ensure PII is not posted.
6. Eliminate the use of Social Security Numbers (SSNs). All commands must provide the NSTC PAC with written justification for using all or any portion of SSNs. If use has been approved, use no more than the last four SSN digits.
7. Ensure PII is not stored in public e-mail folders or on shared drives that do not restrict access to those with an official need to know that information.
8. Ensure individuals who use BlackBerries®, laptops or other portable electronic devices or equipment have been properly trained on how to protect against inadvertent disclosure of PII and of any limits or restrictions on the amount of any PII that can be stored or located on such equipment or device.
9. Remove PII from documents prior to posting or circulating them to individuals who do not have an "official need to know."
10. Assess risks for potential compromise of PII in all files, databases, and other formats to ensure proper safeguards are in place to prevent unauthorized disclosures. Review and update safeguards periodically.
11. Ensure documents of disestablished or transient activities are disposed of as required by reference (d) and are not disposed of in containers subject to public access or compromise.

12. Ensure recycling is accomplished in a manner that does not compromise PII.

13. Shred, all documents in accordance with reference (c) on a daily basis, using a cross-cut shredder whenever possible.

14. Ensure compliance with the safeguards listed for each Privacy Act System of Records notice maintained. See www.privacy.navy.mil for a listing of all such Navy notices.

15. Build a Privacy Team of records managers, public affairs officials, IT professionals, legal officers, systems managers, and your Privacy Act officer to discuss ways to implement effective privacy practices.

Employee's Certificate of Initial/Annual Refresher Training

This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities on the date indicated below. I understand that I am responsible for safeguarding Personally Identifiable Information (PII) that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard PII, for improperly using or disclosing such information, and for failure to report any known or suspected loss of the unauthorized disclosure of such information.

(Employee or Trainer's Signature)

(Print Employee's Name)

(Date)

(DoD Component/Office)