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

NSTCINST 5211.1C
OGC
13 Jun 23

NSTC INSTRUCTION 5211.1C

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 System of Records
(2) Best Practices Protocol for Printed and Electronic Media
(3) NSTC PII Spot Check memo

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 (NSTC).

2. Cancellation. NSTCINST 5211.1B.

3. Background. Reference (g), promulgated within the Department of the Navy (DON) by reference (a), requires Federal 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 references (a) and (d).

5. Action.

a. Office of General Counsel (OGC): The NSTC OGC is designated as the NSTC Privacy Act Coordinator (PAC) to perform the duties in paragraph 7(h) of reference (a), for all NSTC commands and activities. As such, the PAC is the principal point of contact (POC) for all PA matters, including but not limited to: reporting Personally Identifiable Information (PII) breaches and acting as the POC for all follow-up actions and individual notifications regarding any breach. Commands and activities subordinate to NSTC must contact the NSTC PAC in the event of any actual or suspected PII breach and shall act only through the PAC. NSTC PAC has designated a group email, NSTC_GRLK_PRIVACY@us.navy.mil, where PII breaches and PII Spot Checks can be sent. The NSTC PAC shall

(1) Provide assistance when notified by a command, activity, department, or PA System Administrator of the need to establish a new System of Records or amend, alter, or delete an existing System of Records. NSTC OGC shall notify and coordinate all such changes with Director, Navy Staff (DNS-36). Current Systems of Records used by NSTC are listed at enclosure (1);

(2) Provide training to NSTC Command Duty Officer (CDO) regarding the loss or suspected loss of PII, including the completion of the DD2959 form; and

(3) Semi-annually in May and November, coordinate a command-wide review of NSTC PA practices 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 approved and provided by the PAC. 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; and

(c) Identification in writing of all currently appointed PA Office Administrators (previously designated as PA POCs) and any System of Records Administrators.

b. NSTC Command Information Officer (CIO)(N6) shall.

(1) Provide guidance for effective assessment and utilization of privacy-related technologies;

(2) Develop and coordinate privacy policy, procedures, education, training, and awareness practices regarding NSTC information systems;

(3) Provide guidance to properly protect PII on portable storage devices and ensure portable storage devices do not contain any PII unless properly protected pursuant to that guidance;

(4) Provide guidance to System of Records Administrators on the conduct of Privacy Impact Assessments (PIAs) of NSTC information systems;

(5) Oversee 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;

(6) Review all NSTC PIAs prior to requesting approval by the chain of command (NETC CIO or OPNAV N15B) as required;

(7) Ensures NSTC compliance with DON information systems privacy requirements, including the use of encryption software and implementation of prescribed privacy-related technologies; and

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

c. NSTC Public Affairs Officer (PAO). The NSTC PAO shall ensure NSTC compliance with DON World Wide Web privacy requirements.

d. Commanding Officers (CO), Directors, Department Heads, and Special Assistants (DD/SA). CO's and DD/SAs shall:

(1) When the CO of Recruit Training Command, CO of Officer Training Command, or DD/SAs within NSTC is notified of a loss or suspected loss of PII, they shall notify DON CIO of the discovery of a loss or a suspected loss of PII via form DD2959. When the CO of a Naval Reserve Officers' Training Corps (NROTC) unit is notified of a loss or suspected loss of PII, the NROTC CO shall complete form DD2959, submit it to US-CERT, the DON CIO Privacy Office, OPNAV 6, and CHINFO by clicking the appropriate button on the form, notify the NSTC PAC, and provide the PAC with a copy of the completed DD2959. Send copy to NSTC_GRLK_PRIVACY@us.navy.mil;

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

(3) Appoint a PA Point of Contact (PA POC) in writing that clearly defines the PA POC'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: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/NavyUSMC- Article-List/;

(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;

(6) Ensure that only DON personnel with a "need to know" in the official performance of their duties have access to information contained in a System of Records;

(7) Advise contracting officers and the PAC of any violations or deficiencies by contractors in regard to the Privacy Act or the Protection of PII;

(8) Have all information reviewed for PII by the NSTC PAO before placing it onto the NSTC or Officer Training Command Newport command websites. Recruit Training Command (RTC) shall have the RTC PAO review and approve information before it is placed on the RTC website. These PAO reviews include a review for PII. Any Naval Reserve Officers Training Corps unit's website shall contain a disclaimer that is not an official DON website;

(9) Ensure their personnel who deal with PA receive initial PA training within 30 days of employment with the command and annual refresher training thereafter. A record of initial and annual refresher training shall be maintained for two years after the date of training;

(10) Ensure portable storage devices do not contain any PII unless the information is properly protected pursuant to guidance issued by the NSTC CIO;

(11) Semi-annually, in May and November, 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. A PII Spot Check Form approved by the PAC shall be used to conduct this review;

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

(13) Follow the best practices set forth in enclosure (2). These are intended to be a starting point and are not to be regarded as an exhaustive list of all possible best practices; and

(14) Designated PA Office Administrator in writing with copies sent to PAC.

e. NSTC CDO shall: The NSTC CDO shall, when notified of a loss or suspected loss of PII, complete a DD2959 and submit it to US-CERT, the DON CIO Privacy Office, OPNAV N6, and CHINFO by clicking the appropriate button on the form, notifying the NSTC PAC, and providing the PAC with a copy of the completed DD2959.

f. System Administrators. 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; and

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

g. Command Assessments/Inspector General shall: Conduct staff assistance visits or program evaluations within NSTC and lower echelon commands to ensure PA compliance.

h. All NSTC Personnel shall:

(1) Ensure portable storage devices do not contain any PII unless the information is properly protected, pursuant to guidance issued by the NSTC CIO

(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 Department of Defense (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) Take every step to properly mark correspondence so the recipient is aware of the need to properly protect the information in those instances where transmittal of PII is necessary. When mailing PII, double wrap the contents, and address the internal wrapper o the intended recipient and mark it "CUI" at both the top and the bottom of the page. Electronic transmissions shall be encrypted and password protected;

(7) Not maintain privacy sensitive information in public folders, whether in hard copy or online;

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

(9) Immediately report maintenance of any unauthorized System of Records to the PAC; and,

(10) Dispose of records from Systems of Records in accordance with all applicable guidance, including the System of Record 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 crosscut 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 irretrievable 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 PA, and requested for release within DoD shall be released only to those with a need to know. All requests for a 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.

7. Privacy Act Team. A Privacy Act Team (PA Team) consisting of the NSTC Chief of Staff (CoS), PAC, IG, Administrative Officer, PAO, (CIO), and others as assigned by the CoS, shall meet as needed. The PA Team shall:

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

b. Review self-assessment reports for NSTC and NSTC commands and activities. Following this review, the PA Team shall recommend modifications or revisions to documents and procedures, as appropriate.8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.l January 2012.

9. Review and Effective Date. Per OPNAVINST 5215.17A, OTCN will review this instruction annually on the anniversary of its effective date to ensure palpability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction.

Craig T Mattingly
C. T. MATTINGLY

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Naval Service Training Command issuance website,
http://www.netc.navy.mi1/nstc/NSTC_Directives/instructions.html.

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 N05354-1 Equal Opportunity Management Information System
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

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.

4. Be certain that PII is not left unprotected and visible on desktops, 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. Minimize or eliminate the use of Social Security Numbers (SSNs). All commands must provide the NSTC PAC with written justification for using SSNs, and if use has been justified, they must truncate the SSN to no more than the last four 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 crosscut shredder whenever possible.

14. Ensure compliance with the safeguards listed for each Privacy Act System of Records notice maintained. See https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/NavyUSMC-Article-List/ 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.

This page intentionally left blank

NSTC PII Spot Check memo

From: ________________________________(DEPARTMENT OR COMMAND)
To: NSTC Privacy Act Coordinator

Subj: PII SPOT CHECK FOR ____________(MONTH AND YEAR)

This memorandum is an internal document and is to be used by activity 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 or (DSN 792). This memorandum is an auditable record and must be kept on file for two years after it is compiled.

Administrative

1. The name of my PA Office Administrator is ____________________________.

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

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 5211.1B, NSTC Command Privacy Act Program or does the activity believe additional guidance is necessary? If so, please explain.

4. Has the activity implemented Privacy Act guidance additional to that issued in NSTC INSTRUCTION 5211.1B, NSTC Command 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 contains 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. Not Applicable

Paper Records

9. At random, spot check 10 percent of locked bins/file cabinets 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.

a. Number of locked bins checked________ b. Number of locked bins containing PII ________
c. Not Applicable □

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

a. Number of containers checked _______ b. Number of containers containing PII_________
c. Not Applicable □

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

a. Yes □ b. No □ c. Not Applicable □

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

a. Yes □ b. □

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.

a. Number of boards checked _________ b. Number of times where PII was found _________
c. Not Applicable □

Electronic Record/Hardware

14. Per reference (b), written procedures for laptops and portable electronic equipment have been created and implemented for 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 devices not in compliance __________
c. Not Applicable □

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.

a. Number of files containing PII _______b. Number of files not encrypted ______
c. Not Applicable □