DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS MARYLAND 21402-1300

USNAINST 5211.3B
28/AO
21 SEP 2011

USNA INSTRUCTION 5211.3B

From: Superintendent

Subj: PROTECTING INDIVIDUALS' PERSONAL RECORDS UNDER THE PRIVACY ACT

Ref: (a) SECNAVINST 5211.5E
(b) SECNAVINST 5720.42F
(c) 5 USC § 552a, Privacy Act
(d) ALNAV 042232Z of Oct 07
(e) USNAINST 5213.2F
(f) SECNAVINST 5210.8D

Encl: (1) U.S. Naval Academy Forms Requiring a Privacy Act Statement
(2) System of Records Used at the Naval Academy and System Custodians
(3) Personally Identifiable Information Spot Check Form

1. Purpose. To carry out the provisions of the Privacy Act (PA) as implemented in reference (a) and increase awareness of the need to protect personally identifiable information (PII).

2. Cancellation. USNA Instruction 5211.3A. This instruction has been completely revised and should be read in its entirety.

3. Background

a. Reference (a) implements the PA throughout the Department of the Navy (DON) and:

(1) Delineates revised policies and procedures which govern the collection, safeguarding, maintenance, use, amendment, and dissemination of personal information retained by the DON in a system of records (SOR) from which information is retrieved by a personal identifier. Personal information is described in reference (a).

(2) Prescribes:

(a) Procedures for disclosing PII.

(b) Procedures for verifying the identity of individuals who request their records.

(c) Procedures for granting individuals access to their records.

(d) Procedures for reviewing a request from an individual who wishes to amend their records, for making determinations on those requests, and for appealing adverse determinations.

(e) Procedures for notifying the public of the existence and character of each system of records notice (SORN).

b. Reference (b) implements the Freedom of Information Act (FOIA) throughout the DON and prescribes policies and procedures for response to requests for access to records other than those records pertaining to the requestor (considered a FOIA request).

4. Applicability. Reference (a) applies throughout the DON, including USNA, for maintaining SORs to accomplish DON missions. This instruction applies to all SORs maintained at USNA from which

information is retrieved by the name of the individual or by some other identifying particular assigned to the individual. It also applies to all requests for notification concerning, access to, or amendment of records within such system.

5. Policy, Responsibilities, and Authority

a. Policy. Subject to provisions of reference (a) and this instruction, USNA policy is to:

(1) Safeguard PII by establishing appropriate administrative, technical, and physical safeguards to ensure that the records in every SOR are protected from unauthorized alteration or disclosure, thereby protecting their confidentiality; and protect the records against reasonable anticipated threats of hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

(2) Protect the privacy of individuals from unwarranted invasions by ensuring all personnel comply fully with references (a) and (b) and this instruction.

(3) Collect, maintain, and use only that personal information needed to support a USNA function or program as authorized by law or Executive Order, and, disclose this information only as authorized by reference (a) and this instruction.

(4) Keep only personal information which is timely, accurate, complete, and relevant to the purpose for which it was collected.

(5) Permit individuals to access or obtain certain copies of any or all portions of their records, subject to exemption procedures authorized by reference (a).

(6) Ensure when discrepancies are proven to be erroneous, untimely, incomplete, or irrelevant, permit individuals the opportunity to request an amendment to their records.

(7) Permit individuals an opportunity to request an administrative review of decisions which deny them access to, or which refuse to amend their records.

(8) Ensure adequate safeguards are enforced to prevent the misuse, unauthorized disclosure, alteration, or destruction of personal information in records.

(9) Maintain no records which describe how an individual exercises rights guaranteed by the First Amendment (freedom of religion, speech, and press; peaceful assemblage; and petition for redress of grievance).

(10) Only maintain SORs which have been published in the Federal Register.

b. Responsibilities

(1) Privacy Act Coordinator (PAC). The Superintendent's Administrative Officer is designated as the PAC for the USNA and will serve as the principal point of contact on all PA matters. On the occasion of the PAC's relief, this designation shall be a part of any turnover. The PAC shall:

(a) Provide training for activity/command personnel in the provisions of reference (a). Report completion of annual training to the Flag Secretary.

(b) Issue implementing instructions.

(c) Review internal directives, practices, and procedures, including those for forms and records, for conformity with reference (a) and this instruction.

(d) Compile and submit input for the quarterly privacy act report to the Chief of Naval Operations.

(e) Maintain liaison with records management officials for maintenance and disposal procedures for standards, forms, and reports as set forth in reference (a).

(f) Conduct semi-annual spot checks and site visits/evaluations.

(g) Maintain auditable records for spot checks, training records, and on site evaluations. Records shall be submitted to the Flag Secretary annually for audit.

(2) Denial Authorities. Per reference (a), the Superintendent is designated as a denial authority and is authorized to deny requests for notification, access, and amendment when the records relate to matters within his area of command, technical, or administrative responsibility, as appropriate. The PAC is authorized to act as a denial authority and to sign "By direction" correspondence relating to routine PA matters.

(3) Granting Authority. The Superintendent is the System Manager for all SORs maintained at the Naval Academy and, as such, is responsible for granting the notification, access, and amendment requests governed by reference (a). The PAC is authorized to act by direction of the Superintendent in this regard. A request governed by reference (a) and this instruction may be granted by the PAC.

(4) Systems Custodians. A systems custodian is the individual responsible for ensuring PII being collected on a particular SOR is following regulations established in reference (a), the applicable SORN, and this instruction. SORs maintained at USNA are listed in enclosure (2) and are accompanied by their designated systems custodian. Report additions or deletions to PAC at nye@usna.edu. Systems custodians shall:

(a) Provide the PAC the system custodian, by name, responsible for the SOR and SORN execution within 10 days of receipt of this instruction. These individuals are responsible for conducting semi-annual spot checks during the first week in September and March. They shall document completion on enclosure (3) and deliver the completed form to the PAC by the 15th of each month to be retained as auditable records.

(b) Ensure all personnel collecting PII in their department have had annual training on the Privacy Act.

(c) Ensure all personnel having access, in any way, to the SOR or who are engaged in the development of procedures or handling records are knowledgeable of the requirements in reference (a) and this instruction and any safeguarding or maintenance procedures unique to their SOR.

(d) Allow individuals to have access to and/or make copies of their records to which they are entitled. Individuals can request access to a SOR pertaining to themselves that are maintained by the DON, including USNA. Individuals should submit requests using the guidelines provided at http://www.privacy.navy.mil.

(e) Ensure a SORN has been published in the Federal Register and any additions or significant changes are prepublished in the Federal Register. Maintaining an unpublished SOR constitutes a criminal violation under subsection i(2) of 5 U.S.C. § 552a and reference (a).

(f) Ensure records are kept in accordance with retention disposal requirements set forth in references (a) and (f).

(g) Evaluate information proposed for each SOR for relevance and necessity. Review annually each USNA SOR and SORN to determine if the records are up-to-date and/or used in matching programs and whether they are in compliance with the OMB Guidelines.

(h) Keep the PAC informed of non-routine PA requests.

(i) Review enclosure (2) and report any SOR being used or maintained at USNA which is not listed in enclosure (2). SORs maintained under the DON's umbrella, can be viewed at http://dpclo.defense.gov/privacy/SORNs/component/navy/index.html.

(j) Ensure forms posted online have an approved USNA form number and are prepared in accordance with (IAW) reference (e).

(k) Ensure procedures for disposal of PII are routinely reviewed and disposed of IAW reference (f).

(5) Automatic Data Processing (ADP) Security. The Deputy for Information Technology is designated as the USNA ADP Systems Security Officer and is responsible for securing, monitoring, and controlling the access of computerized files containing personal information.

6. Action

a. General. Although work generated on a government computer is considered FOR OFFICIAL USE ONLY (FOUO), it is not all privacy sensitive (PS). **Do not routinely use as part of your electronic signature** the FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE statement. If you are actually generating an email that contains FOUO – PS information, your subject line should read: FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE followed by the subject. The individual receiving your email needs to know, prior to opening the email, that the information contains FOUO PS information so it can be properly safeguarded.

(1) All letters, memoranda, faxes, notices, etc., containing PII, must have the following legend posted at the bottom of the document ½" from the bottom of page:

FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE
Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.

(2) Do not post PII on a public web site.

(3) Folders being routed through the chain of command which contain PII shall have a label in the upper right hand corner, under the subject label, typed or stamped in red, containing the FOUO - PS statement.

(4) All requests governed by reference (a), and this instruction, regardless of where or how received within the command, shall be forwarded immediately to the PAC, at mail stop 1e, located in the Administrative Building, Room 110. Routing of correspondence in connection with the PA shall be hand carried or forwarded in a double sealed envelope with the inner envelope stamped with the FOUO - PS statement. Yard mail envelopes may be used for the outer envelope with a sealed envelope inside. Do not stamp the FOUO – PS statement on the outside wrapper.

(5) Enclosure (1) is a list of USNA forms requiring a privacy act statement (PAS). Review all forms used to collect PII to ensure they contain a PAS.

b. PAC. Upon receipt of a PA request, the PAC shall:

(1) Enter all PA first-party access requests into a tracking system and assign a case number.

(2) Send letter acknowledging receipt of letter within 10 work days and respond to the request within 20 days.

(3) Assist the System Custodian as necessary in responding to the request.

(4) Determine whether fees are to be charged as outlined in reference (a).

(5) Conduct an annual review of all SORs to ensure they are in compliance with current regulations. Per reference (a), advise CNO (DNS-36) promptly of the need to establish a new Navy PA SORN; amend or alter an existing Navy SORN; or delete a Navy SORN that is no longer needed.

(6) Within one hour of the discovery of a loss or suspected loss of PII, notify the United States Computer Emergency Readiness Team.

(7) Per reference (a), ensure all USNA employees receive annual PA training.

c. Employees. Each employee of the Naval Academy has responsibilities for safeguarding the rights of others. Per reference (a), employees shall:

(1) Take annual PA training posted on USNA training site. A notice will be sent out annually announcing the training site and timeframe required for completion.

(2) Not disclose any information contained in a SOR by any means of communication to any person, or agency, except as authorized.

(3) Safeguard the privacy of individuals and confidentiality of personal information contained in a SOR.

(4) Familiarize themselves with reference (a), this instruction, Privacy Act laws, regulations and policies, and understand the ramifications of incorporated access and disclosure. Reference (c) prescribes criminal penalties for violation of PA provisions. Per reference (a), any member or employee of the DON may be found guilty of a misdemeanor and fined not more than $5,000 for willfully:

(a) Maintaining a SOR without first meeting the public notice requirements.
(b) Disclosing information protected under the PA to any unauthorized person/agency.
(c) Obtaining or disclosing information about an individual under false pretenses.

(5) Routinely review the DOD website at http://www.privacy.navy.mil for updates and changes to PA protocols.

7. Upon receiving a PA request for action, the action office shall:

a. Within seven work days, review the PA request and the records concerned; make an initial determination whether the request should be granted or denied in whole or in part, and fill out a DD Form 2086 showing cost estimate for processing the request. Forward the DD Form 2086 to the PAC.

b. Prepare a proposed response within 15 days of receiving the PA request.

c. Forward the proposed response, with appropriate enclosures, to the PAC for approval and release. Send electronic file to admin-routing@lists.usna.edu.

8. Remember if you work with PII, you are responsible to protect everyone's privacy. Protecting an individual's privacy is everyone's business.

/S/
S. S. VAHSEN
Chief of Staff

Distribution:
All Non Mids (electronically)

FORMS REQUIRING PRIVACY ACT STATEMENT

Form Number	Title
USNA 7200/12 (7-11)	United States Naval Academy Foreign National Information
USNA AA 1531/12 (3-11)	USNA Sponsor Application
USNA AA 5500/31 (2-11)	Request for Bancroft Hall Access
USNA BBA 1050/3 (3-08)	Separation Leave Request
USNA BBA 1301/8 (2-07)	Graduation Information/TAD Assignment Sheet
USNA BBA 1920/60 (3-08)	Midshipmen Summary Sheet for Resignation
USNA BBA 1920/61 (3-08)	Evaluation for Consideration for Other Future Officers Training
USNA BBA 5210/11 (8-07)	Midshipman Performance Jacket Record of Disclosure
USNA BBE 1920/62 (3-08)	Chaplain's Interview Sheet
USNA BE 1110/95 (7-11)	USNA Summer STEM Application
USNA CA 11100/5 (11-10)	Special Power of Attorney
USNA CA 11100/6 (11-10)	Release From Liability & Waiver of Claims
USNA CCA 1531/06 (08-93)	Roll Book
USNA CCA 1531/29 (06-06)	Midshipmen Record Change Card
USNA CEA 5720/1 (6-96)	Registration Record-Parents' Weekend
USNA CFB-1531/04 (11-93)	Personal Data for Chemistry Majors
USNA CHA-1520/03 (10-90)	Paper Topic Selection for NAVFAC Conference
USNA CHA 5050/4 (11-90)	Transportation Form
USNA CHB-1531/07 (08-89)	Request for Revocation of Language Validation
USNA CHB-1531/08 (08-89)	Interview Evaluation Points
USNA DH 4001/23 (9-10)	Gift Offer/Acceptance
USNA DH 7200/10 (5-10)	Government Purchase Card Program Convenience Check
USNA DH 7300/13 (4-10)	Payment of Honoraria for Invited Non-Government Guests
USNA DMB 1070/07 (02-92)	Officer Data Input Record
USNA EB 12000/1 (2-06)	Civilian Emergency Contact
USNA ED 1110/08 (3-10)	Naval Academy Information Program Blue & Gold Officer Application
USNA ED 1110/94 (3-10)	Request to Perform Direct Support (IDT/IDTT/AT/ADT) with the Naval Academy Information Program Memorandum
USNA ED 1531/07 (3-10)	Reserve Naval Academy Information Program USNR/USMCR Officer Participation Authorization Request
USNA ED 1650/6 (3-10)	Reserve NAIP Navy Recruiting Service Ribbon Request
USNA ED 1800/06 (3-10)	Retirement Credits Report (Monthly)
USNA ENA-4001/03 (08-88)	Certification for Memorial Gift Fund
USNA FPA 1710/28 (7-98)	Navy Track Questionnaire
USNA GRB-1110/11 (12-06)	Candidate Activities Record

Form Number	Title
USNA GRB-1110/12 (12-06)	Candidate Personal Data Record, Academic Interest, Current Studies & Personal Statement
USNA GRB-1110/14 (12-06)	School Official's Evaluation of Candidate
USNA GRB-1110/15 (12-06)	Request for Secondary School Transcript
USNA GRB-1110/19 (04-01)	Candidate Notice of Withdrawal
USNA GRB-1110/20 (04-01)	Candidate Change of Address Record
USNA GRB 1110/91 (12-06)	Candidate Fitness Assessment
USNA GRB 1110/92 (12-06)	USNA Request for Information
USNA GRB 1110/93 (12-06)	USNA Summer Seminar Application
USNA GRB 1531/34 (12-06)	USNA Preliminary Application
USNA GRB 5050/1 (4-05)	USNA Admissions Outreach Conference Registration
USNA GRD 1110/5 (6-04)	ROTC Nomination to USNA
USNA GRD-1110/15 (06-90)	Candidate Information Release
USNA GRD-1110/16 (08-95)	Certificate of Acceptance/Declination
USNA GRD-1110/21 (5-99)	Requesting a Presidential Nomination
USNA GRD-1531/08 (11-89)	Oath of Office for Foreign Students
USNA GRD 5500/1 (8-01)	Police Record Check
USNA GRE 1110/7 (2-09)	Fulfill Your Destiny
USNA GRE 1110/08 (09-99)	Naval Academy Information Program Affiliate Application
USNA GRE 1110/56 (3-02)	Fleet Orders Acceptance for NAPS
USNA GRE 5512/4 (3-02)	Naval Academy Summer Seminar Vehicle Access
USNA MMA 1301/4 (7-11)	Ensign Detachment Request
USNA MMD 1730/8 (11-07)	Application for a Wedding Ceremony
USNA NB 4650/4 (2-09)	Commercial Travel Reservation for Group Travel
USNA NNB 4650/3 (2-07)	Creating Employees (Military & Civilian) In DTS
USNA NNB 4650/4 (2-07)	Government Travel Charge Card Program New Employees (Military & Civilian) Transferring to USNA
USNA NNB 7420/16 (2-07)	Request for Change of Address
USNA PYA 5720/3 (6-03)	Midshipman Publicity Background Record
USNA RKA 1730/2 (6-00)	Wedding Music - Pink
USNA TWA 10170/1 (4-94)	Sailing Equipment Custody Record
USNA UUA 3172/2 (10-08)	YP Usage Request
USNA VVA-12600/11 (08-89)	Personnel Absence & Leave Record

SYSTEMS OF RECORDS USED AND MAINTAINED AT USNA

ID #	System Name	System Custodian
DHRA 08 DoD	Defense Travel System (March 24, 2010, 75 FR 14142)	Comptroller
GSA/GOVT-3	Travel Charge Card Program (January 30, 2004, 69 FR 4517)	Comptroller
GSA/GOVT-6	GSA SmartPay Purchase Charge Card Program (November 3, 2006, 71 FR 64707)	Comptroller
N01070-3	Navy Military Personnel Records System	Personnel Officer Midshipmen Personnel Officer
N01080-1	Enlisted Master File Automated Systems	Personnel Officer
N01080-2	Officer Master File Automated Systems	Personnel Officer
N01131-1	Officer Selection and Appointment System	Personnel Officer
N01531-1	USNA Applicants, Candidates, and Midshipmen Records	Dean of Admissions Director, Candidate Guidance Head, Nominations & Appointments Academic Dean & Provost Registrar Director, Professional Development Performance Officer Midshipmen Information Systems Officer Midshipmen Personnel Officer Sponsor Director
N01770-3	Naval Academy Cemetery and Columbarium Records	Memorial Affairs Coordinator
N05041-1	Inspector General Records	USNA IG
N05300-3	Faculty Professional Files	Academic Dean
N05350-1	Navy Drug and Alcohol Program System	Commandant of Midshipmen Human Resources Department
N05354-1	Equal Opportunity Management Information System	Deputy, Equal Employment Opportunity Officer
N05520-5	Personnel Security Program Management Records System	Security Manager ITSD Senior Message Center Person
NM01500-2	Department of the Navy (DON) Education and Training Records	Academic Dean
NM01650-1	Department of the Navy (DON) Military Awards System	Personnel Officer

ID #	System Name	System Custodian
NM05000-1	General Correspondence Files	Administrative Officer Archives All Division Directors All Department Heads
NM05000-2	Organization Management and Locator System	Superintendent All Division Directors All Department Heads
NM05211-1	Privacy Act Request Files and Tracking System	Privacy Act Coordinator
NM05512-2	Badge & Access Systems Records	ATFP Assistant
NM05380-1	Combined Federal Campaign/Navy and Marine Corps Relief Society	Chairperson, Combined Federal Campaign Chairperson, Navy and Marine Corps Relief Society
NM05720-1	FOIA Request/Appeal Files and Tracking System	FOIA Coordinator
NM07010-1	DON Non-Appropriated Standard Payroll System	HR Assistant/Payroll Administrator for NABSD
NM07421-1	Time and Attendance Feeder Records	Comptroller Timekeepers
NM12610-2	Hours of Duty Records	Director, Human Resources Officer Personnel
NM12630-1	Voluntary Leave Transfer Program Records	Director, Human Resources
OPM/GOVT-1	General Personnel Records	Director, Human Resources
OPM/GOVT-2	Employee Performance File System Records	Director, Human Resources
OPM/GOVT-3	Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers	Director, Human Resources
OPM/GOVT-4	File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints	Director, Human Resources
T7225	Integrated Accounts Payable System (IAPS) (May 4, 2007, 72 FR 25271)	Comptroller
T7335	Defense Civilian Pay System (DCPS) (December 12, 2008, 73 FR 75683)	Comptroller

PERSONALLY IDENTIFIABLE INFORMATION (PII) SPOT CHECK

This document will be used, by system custodians, to assess the level of compliance in handling of PII as delineated by law and or specific DoD/DON policy guidance. For additional guidance and information, contact the Privacy Act Coordinator (PAC) at x31550. This form is an auditable record and shall be kept on file for three years by the PAC.

PII is information that carries some risk-of-harm to an individual, or to the command, if the information is accessed by unauthorized personnel. PII is considered "sensitive" and must be protected. Sensitive PII includes, but is not limited to, Social Security Number, personal medical information, and financial information.

PII that is releasable to the public in accordance with law (5 USC 552), regulations (5 CFR 293.311 or 32 CFR 310.22), or commonly used in the work environment (OSD 15041-07), is not considered to be of risk to an individual nor command. All non-sensitive PII must be examined in its context of use. Context of use can make non-sensitive PII (a list of 'just names') sensitive if the list is contextually associated with sensitive information (list of 'just names' in a folder marked "Employees who failed a drug test").

The following PII is normally considered to be not sensitive for all employees and contractors: name, work phone, work email, code, rank, work location, and assigned position.

ADMINISTRATIVE

1. Name of individual assigned to conduct this spot check is _____.

2. Area of responsibility checked (Bldg/Floor) _____.

(Department) _____.

3. Date spot check conducted _____.

PAPER RECORDS

1. Has your area of responsibility developed a PII records disposal program? _____.

2. Number of personnel in department _____. Number of personnel that received PII training in last 12 months _____.

Ref: GENADMIN: DON CIO WASHINGTON DC 181905Z DEC 08

3. Number of PII breaches reported this calendar year _____. Number of personnel notified _____.

4. Spot check 10% of recycle containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal.

Ref: SECNAVINST 5211.5E

Number of containers checked _____. Number of containers containing PII _____.

5. Spot check 10% of waste containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal.

Ref: SECNAVINST 5211.5E

Number of containers checked _____. Number of containers containing PII _____.

6. For static bulletin boards disseminating/displaying information, check for the presence of PII.

Ref: SECNAVINST 5211.5E

Number of boards checked _____. Number of examples of where PII was found _____.

ELECTRONIC RECORDS/HARDWARE

1. For Non-NMCI networks: Is your activity currently using "Mobile Armor" to protect DAR on non-NMCI laptops, desktops and removable storage media? If no, when will a DAR product be implemented? If using other than Mobile Armor, provide date that a DON CIO waiver was granted? _____.

Ref: GENADMIN: DON CIO WASHINGTON DC 181905Z DEC 08

2. Has a check in/check out log for all laptops and portable electronic equipment been created and implemented for all such devices that contain PII on >24 individuals and that are transported outside a secure government space. Does the supervisor maintain this log and can it be produced upon request?

_____. Supervisor's name and extension. _____.

Ref: DONCIO 171952Z APR 07

3. Spot check at least 10% of laptops within your area of responsibility. Ensure all data is encrypted, the time out function is enabled and each unit is password protected.

Ref: SECNAVINST 5211.5E

Number of laptops checked _____. Number of laptops not configured as required _____.

4. Spot check at least 10% of PDA/Blackberries within your area of responsibility. Ensure the time out function is enabled and each unit is password protected.

Ref: SECNAVINST 5211.5E

Number of units not in compliance _____. Not applicable, AOR has no PDA's _____.

5. Search and spot check 25% of files on the shared drives within your area of responsibility. Ensure that no PII has been posted.

Number of files checked _____. Number of files containing PII _____.

6. Are all computer hard drives physically destroyed when sent to disposal? _____.

7. Are copier/printer machine hard drives sanitized or destroyed prior to disposal? _____.

WEBSITES

Spot check 25% of your area of responsibility web sites (internal and external), searching for PII that is available to individuals who do not have a need to know.

Ref: SECNAVINST 5720.47B

Number of sites checked _____. Number of records with PII _____. N/A _____.