



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

USNAINST 5211.3D  
28/AO  
17 Sep 18

USNA INSTRUCTION 5211.3D

From: Superintendent, U.S. Naval Academy

Subj: U.S. NAVAL ACADEMY PRIVACY PROGRAM

Ref: (a) 5 U.S.C. §552a  
(b) SECNAVINST 5211.5 (series)  
(c) SECNAV M-5210.1  
(d) USNAINST 5213.2 (series)

Encl: (1) Systems of Records Used at U.S. Naval Academy (USNA) and Associated System Sponsors  
(2) USNA Privacy Program Requirements and Procedures

1. Purpose. To implement USNA Privacy Program per references (a) through (c).
2. Cancellation. USNAINST 5211.3C. This is a complete revision and should be reviewed in its entirety.
3. Definitions. See reference (b) for additional definitions.
  - a. Access. An individual's ability or opportunity to gain knowledge of Personally Identifiable Information (PII) or a record contained in a System of Records (SOR).
  - b. Disclosure. The information sharing or transfer of any PII from a SOR by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, government agency, private entity other than the subject of the record, the subject's designated agent, or the subject's legal guardian.
  - c. PII. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information, that is linked or linkable to a specific individual.
  - d. Privacy Act (PA) Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual that are maintained in a SOR.
  - e. Privacy Impact Assessment (PIA). An assessment throughout the life cycle of Information Technology (IT) systems and electronic collections that collect, maintain, use, or disseminate PII for members of the public or federal personnel. The purpose of the assessment is to evaluate adequate practices and balance privacy concerns with the security needs of an organization.

f. **Public-Facing Website.** A website that's available via the internet from any location as opposed to USNA's intranet that is only accessible with a USNA account while connected to the network.

g. **PA Record.** Any item, collection, or grouping of information, regardless of storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a Department of the Navy (DON) activity that contains the individual's name or other identifying particulars assigned to the individual.

h. **System of Records (SOR).** A group of records under the control of a DON activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual.

i. **System of Records Notice (SORN).** A notice published in the Federal Register that constitutes official notification to the public of the existence of a SOR.

#### 4. Responsibility and Authority

##### a. Superintendent

(1) Per reference (b), the Superintendent is designated as USNA's denial authority and is authorized to deny access to information under the exemptions cited in PA SORNs for PA SOR maintained at USNA. The denial authority may also deny requests to amend a SOR or deny notification that a record exists. The Privacy Coordinator is authorized to act as a denial authority for USNA and the Naval Academy Preparatory School (NAPS).

(2) The Superintendent is USNA's release authority for all PA SOR maintained at USNA. The release authority is authorized to release records requests from non-exempt PA SOR maintained at USNA. The release authority may also grant requests for notification and amendments to a PA SOR. The Superintendent extends release authority to:

(a) The Privacy Coordinator to act on the Superintendent's behalf for all USNA and NAPS PA related matters, and who is authorized to sign "By direction" correspondence using the title Privacy Act Coordinator or Freedom of Information Act Coordinator.

(b) The Registrar for releasing routine requests for academic records and PA records maintained by the Registrar's Office per reference (a).

(c) The Conduct Officer for releasing conduct records to first party requestors and security clearance investigators per reference (a).

(d) The Memorial Affairs Coordinator for releasing records contained in the Naval Academy Cemetery and Columbarium Records SORN per reference (a).

(e) The Staff Judge Advocate (SJA) for releasing records maintained by the SJA's Office.

(f) The NAPS Associate Dean and Registrar for releasing midshipman candidate records maintained by the NAPS Registrar's Office.

(g) Institutional Research for releasing statistics to requesters who have provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record will be transferred in a form that is not individually identifiable.

(h) The Dean of Admissions for releasing admissions records per SORN N01531-1 and to the Department of Homeland Security in response to the requirements of the Student and Exchange Visitor Program.

b. The NAPS Commanding Officer shall:

(1) Designate a Privacy Liaison for NAPS to assist USNA's Privacy Coordinator in carrying out the provisions of this instruction per references (a) through (c).

(2) Serve as a member of USNA's Privacy Act Team.

c. Members of the Senior Leadership Team (SLT). All members of the SLT will serve as members of the Privacy Act Team.

d. Superintendent's Administrative Officer. The Superintendent's Administrative Officer is designated as USNA's Privacy Act Coordinator (PAC) and shall administer the USNA Privacy Program per references (a) through (c), including:

(1) Collecting semiannual spot check forms from System Custodians and maintain them per reference (c).

(2) Providing PII System Custodian training when necessary.

(3) Completing USNA's self-inspection Compliance Spot Check List semi-annually and maintain per reference (c).

(4) Serving as NAPS PAC.

(5) Serve as a member of USNA's Privacy Act Team.

e. Deputy for Information Technology. The Deputy for Information Technology is designated as the Program Manager (PM) in regards to Life Cycle Management per reference (b) and is responsible for providing enabling technology to implement the privacy program and:

(1) Will work with the PAC and PA System Sponsors to update and create PIAs when needed for USNA.

(2) Will ensure only personnel with a need to know and an approved DD Form 2875 have access to USNA PII stored on the USNA network.

(3) Serves as a member of USNA's Privacy Act Team or designate a knowledgeable representative to serve on his behalf.

f. SJA. The SJA serves as a member of USNA's Privacy Act Team.

g. Command Counsel. The Command Counsel will serve as a member of the USNA's Privacy Act Team.

h. Public Affairs Officer (PAO). The PAO serves as a member of USNA's Privacy Act Team.

i. Privacy Act System of Records Sponsors (System Sponsors). System Sponsors, listed in enclosure (1), are responsible for overseeing the collection, maintenance, use, and dissemination of information from a PA SOR, ensuring that all personnel who have access to those records are aware of their responsibilities for protecting PII that is being collected or maintained per reference (b), and:

(1) Providing the Privacy Coordinator with a PII system custodian, by name, responsible for their SOR and updating the Privacy Coordinator if the system custodian turns over.

(2) Reporting all privacy breaches to the Privacy Coordinator within one hour of discovery and assisting the Privacy Coordinator in completing privacy breach actions.

(3) Ensuring PII system custodians perform semiannual spot checks using USNA 5211/1 Naval Academy Personally Identifiable Information Spot Check form and ensuring discrepancies are promptly corrected.

j. PII Custodians. PII custodians are responsible for conducting semiannual spot checks in September and March of each fiscal year. They shall document completion on the form USNA 5211/1 and deliver the completed form to the Privacy Coordinator to be retained as an auditable record.

k. Training Officers and Coordinators. USNA and the Naval Academy Athletic Association (NAAA) training officers and coordinators are responsible for ensuring new employees receive the DON Annual Privacy Training before gaining access to PII in any form or format or gain access to the USNA network. Training is due annually by September 30th of each year with no longer than 12 months between each training.

1. USNA Employees and Contractors. USNA employees and contractors are responsible for safeguarding the rights of others by adhering to the standards set forth in references (a) through (c) and to:

(1) Only collecting and accessing the minimum PII necessary to conduct government business in the performance of their duties.

(2) Only using PII per the purpose of the SORN that authorized the collection of the information and safeguard the information from unauthorized disclosure.

(3) Only collecting PII for inclusion in a PA SOR if there is an approved SORN authorizing the collection of information and per reference (d).

(4) Reporting any loss/breach of PII to supervisor upon discovery.

(5) Completing the DON mandatory annual privacy training before September 30th of each fiscal year through the Total Workforce Management System (TWMS), Navy Knowledge Online (NKO), General Military Training (GMT) provided at USNA, or another supervisor approved means of training.

(6) Familiarizing themselves with and adhere to the privacy program procedures contained in enclosure (2).

m. Contracting Officers. Contracting Officers are responsible for:

(1) Ensuring all contracts where contractors gain access to a government information system or PII include all the required Federal Acquisition Regulation clauses pertaining to privacy.

(2) Ensuring Contracting Officer Representatives are aware of their requirements per this instruction.

(3) Ensure required privacy documents are completed before awarding a contract where PII will be stored on a non-government owned and managed information system, i.e. cloud computing service approval and approved PIA.

n. USNA Contracting Officer Representatives. Contracting Officer Representatives are responsible to:

(1) Informing contractors of their responsibilities regarding USNA's Privacy Program and ensure they adhere to the regulations set forth in this instruction and references (a) through (c).

(2) Ensuring contractors comply with the procedures established by the Defense Acquisition Regulatory Council.

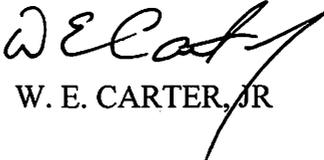
(3) Documenting completion of the annual Privacy and PII Awareness training for each contractor with access to PII and provide documentation to the Privacy Coordinator when solicited.

(4) Ensuring a signed non-disclosure agreement is on file and a DD Form 2875 System Authorization Access Request (SAAR), for each contractor with access to PII.

5. Records Management. Records created as a result of this instruction, regardless of media or format, shall be managed per reference (c).

6. Forms. Form USNA 5211/1 Naval Academy Personally Identifiable Information Spot Check can be found on the USNA Privacy website, <https://www.usna.edu/AdminSupport>, or Naval Forms Online and shall be used for all USNA departmental semiannual spot checks. Forms should be signed and submitted electronically to the Privacy Coordinator at [privacy@usna.edu](mailto:privacy@usna.edu). DD Form 2923 Privacy Act Data Cover Sheet and DD Form 2875 System Authorization Access Request (SAAR) can be found on the DoD Forms Management Program website, <http://www.esd.whs.mil/Directives/forms/>. DD Form 2923 should be turned in to the Information Technology Services Division when completed.

7. Review and Effective Date. The Administrative Officer will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after the effective date unless reissued or otherwise canceled prior to the 5-year anniversary date, or an extension has been granted.

  
W. E. CARTER, JR

SYSTEMS OF RECORDS USED AT USNA AND ASSOCIATED SYSTEM SPONSORS

<u>ID #</u>	<u>System Name</u>	<u>System Sponsors for USNA (NAPS Equivalent positions apply for NAPS)</u>
DHRA 08 DoD	Defense Travel System	Comptroller
DOL/GOVT-1	Office of Workers' Compensation Programs, Federal Employees' Compensation Act File	Human Resources
GSA/GOVT-3	Travel Charge Card Program	Comptroller
GSA/GOVT-6	GSA SmartPay Purchase Charge Card Program	Comptroller
N01070-3	Navy Military Personnel Records System	Personnel Officer MIDN 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
N01420-1	Enlisted to Officer Commissioning Programs	Dean of Admissions
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 Personnel Officer Sponsor Director Aptitude Officer

N01543-1	Explosives Handling Qualification/ Certification Program	ESO
N01740-1	Family Dependent Care Program	Personnel Officer
N01754-4	Navy Family Accountability and Assessment System (NFAAS)	Personnel Officer
N01770-3	Naval Academy Cemetery and Columbarium Records	Memorial Affairs Coordinator
N05041-1	Inspector General Records	USNA IG
N05230-1 Officer	Total Workforce Management Services (TWMS)	Human Resources Training
N05300-X	Faculty Professional Files	Academic Dean
N05350-1	Navy Drug and Alcohol Program System	Commandant Human Resources
N05354-1	Equal Opportunity Management Information System	EEO Officer
N05520-5	Personnel Security Program Management Records System	Security Manager
N06110-1	Physical Readiness Information Management System (PRIMS)	CFL
N07220-1	Navy Standard Integrated Personnel System (NSIPS)	Personnel Officer
N12293-1	Human Resources Civilian Portfolio	Human Resources
NM01500-2	DON Education and Training Records	Academic Dean Personnel Officer
NM01500-10	Navy Training Management and Planning System (NTMPS)	Training Officer
NM01543-1	Explosives Handling Qualification /Certification Program	Explosive Safety Officer

NM01650-1	DON Military Awards System	Personnel Officer
NM01730-1	Navy Chaplain Privileged Counseling Files	Senior Chaplain
NM05000-1	General Correspondence Files	Flag Secretary Archives All Cost Center Heads All Division Directors All Department Heads All Supervisors
NM05000-2	Program Management and Locator System	Superintendent All Division Directors All Department Heads All Supervisors
NM05070-1	Library Patron File	Library Director
NM05100-5	Enterprise Safety Applications Management System (ESAMS)	ESAMS Supervisors
NM05211-1	Privacy Act Request/Amendment Files and Tracking System	Privacy 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	Human Resources Comptroller
NM07320-1	Property Accountability Records	Property Managers
NM07421-1	Time and Attendance Feeder Records Timekeepers	Comptroller

NM12610-2	Hours of Duty Records	Human Resources Officer Personnel Midshipmen Personnel
NM12630-1	Voluntary Leave Transfer Program Records	Human Resources
NM12711-1	Labor Management Relations Records System	Human Resources
NM12713-1	Equal Employment Opportunity (EEO) Complaints Tracking System	Human Resources EEO Officer
NM12771-1	Discrimination Complaints	Human Resources
NM12771-2	Administrative Grievance Files	Human Resources
NM12792-7	Drug-Free Workplace Program Records	Human Resources
OGE/GOVT-1	Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records	Legal Comptroller
OGE/GOVT-2	Executive Branch Confidential Financial Disclosure Reports	Legal Comptroller
OPM/GOVT-1	General Personnel Records	Human Resources All Supervisors
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 All Supervisors
OPM/GOVT-5	Recruiting, Examining, and Placement Records	Human Resources

OPM/GOVT-9	File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints	Human Resources
OSC/GOVT-1	OSC Complaint, Litigation, and Political Activity Files	Human Resources Legal
T7225	Integrated Accounts Payable System (IAPS)	Comptroller
T7335	Defense Civilian Pay System (DCPS)	Comptroller

USNA PRIVACY PROGRAM REQUIREMENTS AND PROCEDURES

1. Personally Identifiable Information. USNA will handle PII according to reference (b) and this instruction.

a. Categories of PII

(1) PII is information which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. If PII is lost, stolen, or disclosed to unauthorized personnel without a need to know, it should be reported immediately (within one hour from discovery) to the USNA Privacy Coordinator.

(a) The following elements are PII whether alone or combined with additional personally identifiable information:

1. Social Security Number (SSN) in any form (full, truncated, masked, etc.)
2. Biometric Identifiers (e.g. fingerprint, DNA, iris scan, etc.)

(b) The following elements are determined to be PII only when grouped with the person's name or other unique identifier (need more than just one element by itself), generally including but not limited to:

1. Driver's license number
2. Passport number
3. Other identification number (not alpha #)
4. Citizenship or legal status
5. Gender (not an identifying title such as Mr., Mrs., Ms., etc.)
6. Race or ethnicity
7. Date and/or place of birth
8. Personal home and cellular telephone numbers
9. Personal email, mailing, and or home addresses (not considered PII when addressing an envelope or package for shipment through the mail)
10. Maiden name or mother's middle name
11. Spouse information

- 12. Marital status
- 13. Child information
- 14. Emergency contact information
- 15. Passwords
- 16. Financial information
- 17. Salary and bonus information
- 18. Medical data and protected health information (protected under the Health Insurance Portability and Accountability Act (HIPAA))
- 19. Law enforcement information
- 20. Employment information or history (not current title, work phone, or work address)
- 21. Education information
- 22. Sensitive duty station
- 23. Military records

(2) Non-sensitive PII is a subset of PII, which if lost, compromised, or disclosed without authorization, even when coupled with name, would not result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Disclosure of non-sensitive PII, as a general rule, should be limited to Department of Defense (DoD) personnel. Generally, breach reports are not required for non-sensitive PII. Non-sensitive PII includes, but is not limited to:

- (a) Name
- (b) Office name and location
- (c) Business telephone number
- (d) Business email address
- (e) Badge number

(f) Job title

(g) Pay grade and rank

(h) Lineal number

(i) DoD ID number / Electronic Data Interchange Personal Identifier (EDIPI) and DoD benefits number

(j) Alpha code or candidate number

b. Exceptions to the categories. In addition to the categories above, the context of the PII may determine whether information is considered PII or non-sensitive PII. A list of employee names that are terminally ill, for example, would be considered PII. Rosters or personnel lists, organizational charts, and recall rosters when disclosed outside the DoD can be considered PII due to the real world threats against DoD personnel. Contact the Privacy Office with any concerns over PII classification.

c. Safeguarding PII. In coordination with the minimum standards of safeguarding PII set forth in reference (b), USNA personnel shall:

(1) Mark all papers, electronic documents (email, letters, faxes, etc.), and physical folders containing PII with the following privacy disclaimer at the bottom of the document ½ inch from the bottom of the page: "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties." (Note: Superintendent routing folders containing PII must have the privacy disclaimer in red in the upper right hand corner on the outside of the folder directly under the folder label: otherwise, use DD Form 2923. At no point should a routing sheet containing PII be affixed to the outside of a routing folder.)

(a) Official correspondence letters in the business style, containing only the name and personal mailing address of the recipient, in the inside address line, do not need the privacy disclaimer unless other PII is included in the letter. (Note: Letters of this nature should still be treated as PII when filing and managing the records, with access on a need to know basis, especially if covered by a system of records notice.)

(b) Never mark the outer envelopes or any shipping containers privacy sensitive or with the privacy disclaimer, even if the content of the envelope contains PII. Only the inner envelopes and internal documents contained in the envelope or shipping container should be marked as PII with the privacy disclaimer.

(c) Emails containing only non-sensitive PII do not require the privacy disclaimer. For example sender's signature blocks (generally containing: name, title, office, business telephone, and email address) do not require the privacy disclaimer. Personal email addresses, when listed

as a list of emails in the body of the email, require the privacy disclaimer, but personal email addresses in the to/from fields of the email do not generally require the disclaimer when sent to personnel with a need to know the content of the email in conducting official business and not being used for commercial or personal reasons.

(d) Label documents and the files or folders containing documents with PII using the Privacy disclaimer, but do not label the outside of the locked filing cabinets or name the electronic files using the privacy disclaimer. USNA wants to safeguard PII, not advertise where PII is being maintained.

(2) Emails

(a) Label all emails containing PII "FOUO-PRIVACY SENSITIVE" in the subject of the email and the file name of any attachments containing PII.

(b) Label the body of any emails containing PII and the body of attachments containing PII with the full privacy disclaimer.

(c) Encrypt and digitally sign all emails containing PII.

(3) Facsimile. USNA personnel shall only use facsimile to transmit PII when absolutely necessary and in compliance with the authorized circumstances prescribed in reference (b). USNA personnel shall use a Privacy Act Cover Sheet, DD Form 2923, and receive confirmation of receipt by the addressee when the facsimile of PII is necessary.

(4) PII Data at Rest. The following provisions pertain to PII stored in electronic form. PII shall not be stored on electronic media for convenience, and shall only be stored on electronic media if storage is a required activity of an individual's assigned billet. When PII storage is required it shall comply with the following restrictions:

(a) PII shall never be stored on personally owned electronic devices or removable storage media.

(b) PII shall not be stored on removable electronic media such as a flash drive or external hard drive unless the device is encrypted and approved by the USNA Configuration Control Board.

(c) Existing PII records should be referenced and used whenever possible. Creating copies of PII should be avoided and shall never be made for convenience. When a copy of existing PII must be created, the creator is the data owner and is entirely responsible for its protection.

(d) The PII data owner is responsible for ensuring that access to stored PII is restricted to individuals having a "need to know."

(e) No part of a filename shall contain PII, and all files containing PII shall include the privacy disclaimer within the document.

(f) PII shall preferentially be stored on the USNA network file storage system whenever this is possible (commonly referred to as the “network file share”). Note: the network file share is neither a user workstation local disk nor a server disk.

(g) If network file share storage is not possible, PII may be stored on a workstation local disk if the individual use case has been approved by the USNA Configuration Control Board. If approved:

1. PII shall only be stored on a Windows workstation, the operating system shall be the enterprise-configured version of Microsoft Windows 10, and the full disk shall be encrypted using Microsoft BitLocker.

2. The end user shall not have administrative rights on the workstation.

(h) Non-sensitive PII, as defined in paragraph (2), may be stored in Google G Suite Drive. When PII is stored in Google G Suite Drive, the file may not be downloaded to or synced to a local workstation disk (e.g., via Google Drive Sync) unless the disk is fully encrypted as above.

(i) Each use case that requires exposing PII through a web page must be approved by the USNA Configuration Control Board.

(j) A file containing PII that is generated through use of a scanner shall comply with the above requirements. This includes PII scanned to Google G-Suite Gmail. Note that email containing PII must comply with Enclosure (2) paragraph 1.c.(2) with respect to labeling

(5) USNA Publically Accessible Websites. PII and non-sensitive PII should not be posted on the USNA Publically Accessible Website with the following exceptions:

(a) The only personnel lists, phone rosters, or organizational charts authorized to be posted on the USNA Publically Accessible Website are those for senior leadership and the professional academic faculty, not support staff, for the purpose of maintaining academic standing. This only authorizes the use of professional information such as name, specialty, and other non-sensitive PII to be posted on the USNA Internet.

1. Support staff and other departments may list contact information on the internet as long as it is generic. (e.g. Admissions Office main office number, not personal numbers and admissions@usna.edu with no personal identifiers)

2. Senior leadership is defined as cost center heads, deans, directors, deputy directors, public affairs officials (personnel designated to interact with the public on behalf of USNA), and their equivalents throughout the Yard.

(b) Biographies and official portraits are only authorized for the senior leadership and academic staff as defined above. Portraits must be head and shoulders only and biographies may not include PII.

(6) Mailing PII

(a) Mailing PII via magnetic tapes, CDs, DVDs, hard drives, or other removable storage media is prohibited unless the data is encrypted.

(b) Double wrapping is encouraged when mailing sensitive PII. The inside container shall be marked with the privacy disclaimer. Never mark the outside container using the privacy disclaimer.

(c) If mailing PII of 25 or more individuals, a mail tracking method must be used (i.e. trackable FEDEX).

(d) Yard mail may be used to send PII as long as an inner envelope is used that is addressed to the recipient, sealed, and the privacy disclaimer is affixed over the seal of the inner envelope.

(7) Official Forms. Official USNA forms are those authorized by the USNA Forms Manager that contain an official USNA form number, a Privacy Act Statement (when required), an Office of Management and Budget (OMB) number and agency disclaimer statement (when required), and conform to Navy forms standards set forth in SECNAV M-5213.1. The USNA Forms Manager has a list of approved USNA forms. All official forms will be listed on Naval Forms Online and the USNA Administrative Department website.

(a) Unofficial forms shall not be used to collect PII.

(b) Forms that collect PII directly from an individual must contain a current Privacy Act Statement; additionally, a current OMB number is required if collecting from the public. See SECNAV M-5213.1 for additional details. (Note: The public is defined as non-military and non-government civilians. Spouses and dependents are considered the public.)

(c) Forms that collect social security numbers (SSN), in whole or part, are prohibited unless required by law, require interoperability with organizations beyond the DON, or are required by operational necessity. A list of acceptable uses can be found on the DON Chief Information Officer website at <http://www.doncio.navy.mil>. A SSN reduction memo, SECNAV 5213/1, is required for all forms collecting the SSN.

(8) Destroying PII. USNA's primary method of disposing of PII is shredding, although burning and pulverizing are authorized.

(a) Shredders must be crosscut and cut particles to conform with reference (b). Recommended shred size is 1 mm by 5 mm for PII. (Note: Crosscut shredders that do not meet emerging standards (shred size) shall be replaced with shredders that meet standard within one year of this published guidance.) The use of a shredder service is authorized according to the following:

1. The service is General Service Approved (GSA).
2. The PII is shredded on site (shredder truck).
3. A certificate of destruction is used to verify disposal.

(b) When burning, PII must be burned so the residue is reduced to white ash. When using burn bags, the burn bags should be secured (according to the same rules as storing PII) until the burn bags are destroyed.

(c) When pulverizing, pulverizers and disintegrators are authorized as long as they are equipped with 3/32 inch security screens.

2. Privacy Act Statements (PAS). A PAS is a statement provided to an individual when the individual is requested to provide PII for possible inclusion in a system of records. A PAS is not required when the information requested is only used to verify the identity of an individual and will not be included in a system of records.

a. The PAS shall appear on all USNA forms requiring the collection of PII at the top of the form, under the title, and consist of the following elements:

(1) Authority: List the SORN number authorizing the system of records in which the information will be maintained, as well as all the specific provision of the statutes, Executive Orders, and agency regulations that authorize the collection of information. (Note: E.O. 9397 (SSN) must be cited if collecting SSN.)

(2) Purpose: Provides the principal purpose for collecting the information; must be in compliance with the SORN purpose but does not have to include all purposes covered in the SORN.

(3) Routine Uses: State who will have access to the information on a routine basis for the stated purpose.

(4) Disclosure: State whether it is voluntary or mandatory for the individual to provide the requested information and the possible effects on the individual if the requested information is

not provided. (Note: It is only mandatory when a Federal law or Presidential E.O. states it is mandatory.)

b. If the information is solicited over the phone, the PAS must be read to the individual providing the information before the information is provided.

c. If the information collection medium is a web based form, such as the admissions application portal, the PAS should be posted on the webpage where the information is being solicited or provided through a well-marked hyperlink to a separate form that can be printed and retained by the individual.

3. Privacy Act Advisory (PAA). A PAA is used when an individual is requested to provide a SSN for identification purposes only and the SSN will not be retained in the system of records. The PAA may be conspicuously displayed in the area where the information is displayed or provided as a written notice. For more guidance on writing and using a PAA, refer to reference (b).

4. System of Records Notice. USNA is responsible for maintaining four SORNs, but per enclosure (1), USNA utilizes and maintains information per many others. To be a system of records, information must be maintained and retrievable by a personal identifier, if the information cannot be retrieved by a personal identifier (such as name, candidate number, alpha, etc.), it does not qualify as a system of records.

a. The following USNA owned System of Record Notices are required to be updated every two years:

(1) N01531-1 "USNA Applicants, Candidates, and Midshipmen Records"

(2) N01770-3 "Naval Academy Cemetery and Columbarium Records"

(3) N01420-1 "Enlisted to Officer Commissioning Programs"

(4) N1200-X "Faculty Professional Files"

b. USNA personnel will adhere to all the standards set forth in the SORNs for all the systems of records used or maintained at USNA.

c. All records containing PII retrieved by a personal identifier must be governed by a SORN; if none exists or one needs to be altered, contact USNA's Privacy Coordinator to establish or amend a SORN per reference (b).

5. Privacy Impact Assessment (PIA). USNA's Accredited Enterprise Education Enclave (AEEE) is the only approved information technology system for use at USNA or NAPS. The AEEE covers the Midshipman Interface Data System (MIDS), the NAPS Scholastic Tracking

Accountability Record system (NSTAR), and the Admissions Information System (AIS) and is covered by an approved PIA authorizing use of the system for PII. If USNA's AEEE PIA needs to be adapted to accommodate growing needs, the USNA Program Manager must be consulted to alter the current PIA or create a new PIA per reference (b). At no time will any USNA or NAPS employee or contractor use an unapproved information technology system to store USNA records.

## 6. Privacy Act Requests

a. Only the designated individuals in this instruction are authorized to release information from a system of records maintained at USNA. Release of this information shall be per the following:

(1) It is a first party request from a requester seeking the requester's own records or the first party has signed a Privacy Act Waiver to release the information to a third party. At no point will anyone release information to a third party without a signed Privacy Act Waiver from the first party.

(2) The request is in writing with either a notarized signature or a signed declaration stating "I certify under penalty of perjury of law that the information above is accurate."

(3) Only the Superintendent or the Privacy Coordinator can deny a Privacy Act request in full or in part. All requests that do not meet the release criteria should be forwarded to the Privacy Coordinator for reply to the requester. (If the request is not in writing or not signed, it is not a proper Privacy Act request and does not need to be forwarded to the Privacy Coordinator for denial.)

(4) The request is answered per the provisions of the Privacy Act, reference (b), and is tracked and retrievable by name; year request filed; serial number of response letter; or case file number.

(5) Each Privacy Act request should be acknowledged within 10 working days and answered within 30 working days.

(6) If a third party request for records is received without a first party Privacy Waiver, it should be immediately forwarded to the Privacy Coordinator for release determination under FOIA.

### b. Making a Privacy Act request for USNA

(1) USNA will not accept telephonic requests; unsigned email, fax, or letter requests; or requests that are neither notarized nor signed with an unsworn declaration.

(2) A privacy act request can be submitted by email, mail, or fax at: [privacy@usna.edu](mailto:privacy@usna.edu); United States Naval Academy, Attn. Privacy Coordinator, 121 Blake Road, Annapolis, MD 21402; or 410-293-2303.

(3) USNA will not honor requests that do not reasonably identify the records being sought or blanket information requests.

7. Disclosure. No record contained in a system of records may be disclosed without a written request unless it meets one of the 12 conditions of disclosure established in the Privacy Act. See reference (b) for details. An unauthorized disclosure of PII from a system of records will be treated as a breach and handled per paragraph 8.

8. Breach Reporting. Any loss of control, compromise, unauthorized disclosure or acquisition, unauthorized access, or similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access to PII is considered a PII Breach.

a. Actions when a PII Breach occurs:

(1) Upon discovery, take immediate actions to prevent further disclosure of PII and immediately report the breach to your supervisor. Do not report the disclosure of non-sensitive PII.

(2) Supervisors should report the breach to the Privacy Coordinator (3-1550 or [privacy@usna.edu](mailto:privacy@usna.edu)) as soon as possible after mitigating the effects of the disclosure, but no longer than one hour after discovery. Report the following information:

(a) Date of incident.

(b) Number of individuals impacted and whether they are government civilians, military, contractors, or private citizens.

(c) Description of the incident, to include the cause or suspected cause of the breach, what PII elements were involved in the breach, was the PII encrypted or password protected, did the individuals seeing the data have a need to know, and did the email (if email related) stay within the USNA network domain.

(3) The Privacy Coordinator will take the required actions to report the incident per reference (b).

(4) If notification is required, the department responsible for the breach is responsible for generating the notification letters for the Chief of Staff's signature within 5 days of receiving notice that notifications are required. The letters must be generated, signed, and mailed within 10 days; the department responsible for the breach will ensure the letters are mailed.

(5) Supervisors of the parties responsible for the breach will provide what disciplinary and/or administrative actions were taken. When notification is required, parties responsible are at a minimum required to retake PII refresher training. Report what actions are being taken within 15 days to the Privacy Coordinator.

b. A list of disciplinary and administrative actions to be taken against those who mishandle PII can be found at the USNA privacy website at <https://www.usna.edu/AdminSupport/index.php>.

9. Privacy Act Complaints. All Privacy Act complaints should be sent to the Privacy Act Coordinator for processing.