USNA INSTRUCTION 5211.3E

From: Superintendent, U.S. Naval Academy

Subj: U.S. NAVAL ACADEMY PRIVACY PROGRAM

Ref: See enclosure (1)

Encl:  (1) References
       (2) Definitions
       (3) USNA Privacy Program Requirements and Procedures

1. **Purpose.** Pursuant to the authority in reference (a), this instruction assigns responsibility and implements references (a) and (b).

2. **Cancellation.** USNAINST 5211.3D. This is a complete revision and should be reviewed in its entirety. NDW-USNA-CCD-1531/09 Transcript Request Form.

3. **Definitions.** Contained in enclosure (2).

4. **Applicability.**

   a. This instruction applies to the U.S. Naval Academy (USNA) and the Naval Academy Preparatory School (NAPS), unless otherwise specified, referred to only as USNA throughout.

   b. For the purposes of reference (a), entities that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of (hereinafter, “maintain”) information on behalf of USNA or operate or use information systems on behalf of USNA, must comply with the privacy requirements in law, Office of Management and Budget policies, Department of Defense regulations, and Department of the Navy policies.

5. **Responsibilities**

   a. Superintendent. Pursuant to reference (c), the Superintendent and the Chief of Staff are designated as USNA’s initial denial authorities (IDA), and are authorized to deny requests for access to information and requests to amend information contained in Privacy Act protected systems of records under USNA control in accordance with references (a) and (d).

   b. Privacy Act Coordinator (PAC). The Superintendent’s Administrative Officer is designated as USNA’s PAC. Pursuant to the authority in reference (c), the PAC is delegated as an Initial Denial Authority and Release Authority for records under USNA control. The PAC will administer the USNA Privacy Program in accordance with references (a) and (b) and:
(1) Release or deny access to privacy act protected records maintained by USNA in accordance with reference (a).

(2) Act as USNA’s representative on behalf of the Superintendent for all privacy related matters, and sign related correspondence using the title Privacy Act Coordinator or Freedom of Information Act Coordinator.

(3) Collect USNA 5211/1 Naval Academy Personally Identifiable Information Spot Check forms from privacy custodians and maintain them for a minimum of three years.

(4) Provide privacy guidance and training as necessary and maintain the USNA privacy website and related content.

(5) Complete USNA’s self-inspection compliance spot check semi-annually.

(6) Provide guidance as necessary to NAPS and maintain NAPS privacy coordinator designation letters and contact information.

(7) Maintain disclosure accounting logs for records maintained in a system of records released by USNA pursuant to sections b(3)-b(12) of reference (a).

(8) Review, submit, and maintain USNA breach reports as required.

(9) Ensure all USNA sponsored System of Records Notices are reviewed annually in accordance with reference (b).

(10) Ensure USNA Privacy Act (PA) complaints are processed, investigated, and resolved or elevated to a higher authority.

c. NAPS Commanding Officer (CO). The NAPS CO will designate a privacy coordinator for NAPS to assist USNA’s PAC in carrying out the provisions of this instruction and references (a) and (b).

d. The NAPS Privacy Act Coordinator (NAPS PAC). The NAPS PAC is responsible for assisting the USNA PAC in carrying out the provisions of this instruction and references (a) and (b) at NAPS and will:

(1) Act as a release authority for Privacy Act records maintained by NAPS.

(2) Maintain disclosure accounting logs for records maintained in a system of records released by NAPS pursuant to sections b(3)-b(12) of reference (a).
(3) Ensure all areas of NAPS conduct semi-annual privacy spot checks utilizing USNA 5211/1 and submit them to the USNA Privacy Act Coordinator to be maintained as an auditable record.

e. Deputy for Information Technology. The Deputy for Information Technology is responsible for providing enabling technology to implement the privacy program and will:

(1) Ensure completion of Privacy Impact Assessments (PIAs) for systems and applications maintained at or by USNA when needed per reference (e).

(2) Ensure only personnel with an approved OPNAV 5239/14 System Authorization Request have access to USNA systems of records or Personally Identifiable Information (PII) stored on the USNA network.

(3) Publish policy prescribing what specific privacy information is allowed to be maintained on Commercial Cloud Services authorized for use at USNA per references (f) and (g).

(4) Ensures protection of PII is integrated into the information system life cycle management process for all USNA IT systems, following reference (h).

f. Cost Center Heads. Cost center heads are responsible for:

(1) Providing the PAC with PII custodians, by name, for all areas in their cost center that maintain PII or systems of records.

(2) Ensuring PII system custodians perform semiannual spot checks utilizing USNA 5211/1 and ensuring discrepancies are promptly corrected.

g. The Legal Office (Staff Judge Advocate and Command Counsel personnel). The Legal Office is authorized to release records under the purview of the Legal Office pursuant to reference (a) sections (b)(3)-(b)(12). The Legal Office has the authority to authorize individuals to release information contained in USNA systems of records in accordance with reference (a) sections b(3)-b(12).

h. USNA and NAPS Registrar Offices. The Registrar’s Office is authorized to validate attendance, dates attended, and status of graduation without a privacy release or waiver. The Registrar’s Office will not release any other information, to include amplifying information about attendance or graduation, without a valid PA waiver.

i. Institutional Research (IR). IR is authorized to release statistics to requesters who have provided USNA with advance adequate written assurance that the record will be used solely for statistical research or reporting record, and the record will be transferred in a form that is not individually identifiable in accordance with reference (a) section (b)(5). Institutional Research
will maintain a log of such disclosures pursuant to reference (a) section (c)(1) and provide it to the PAC when requested.

j. Public Affairs Office (PAO). The PAO is authorized to release information from systems of records maintained at USNA that are a matter of public interest and that would be subject to release pursuant to reference (d). The Public Affairs Officer is responsible for ensuring that all public facing websites maintained by USNA are operated in compliance with the laws and requirements cited in reference (i).

k. PII Custodians. PII custodians are responsible for familiarizing themselves with this instruction and references (a) and (b) in order to conduct semiannual spot checks in September and March of each fiscal year. Custodians must document completion utilizing USNA 5211/1 and deliver the completed form to the Privacy Coordinator to be retained as an auditable record.

l. Supervisors. Supervisors will ensure all their employees understand the requirements of references (a) and (b), this instruction, and must:

(1) Ensure their employees receive privacy training before gaining access to PII, the USNA network, a system of records, or any other government information system;

(2) Ensure their employees meet all privacy training requirements each year as published;

(3) Ensure their employee understand the PII breach reporting process to include how to submit a PII breach report: and

(4) Only approve employee access requests for electronic collections containing PII that they are authorized to grant access to or with authorization from the data owner responsible for the electronic collection.

m. Training Officers and Coordinators. USNA training officers and coordinators are responsible for tracking the completion of required privacy training as published each year.

n. USNA Contracting Officials (Contracting Officers and Contracting Officer Representatives (COR)). In addition to the Contracting Official duties listed in paragraph 8 of enclosure (3) to reference (b), contracting officials will report completion of required contractor privacy training when solicited for spot checks or auditing purposes.

o. Program Managers. Program Managers for USNA sponsored system of records as indicated on the USNA Privacy Program website will carry out the functions of a Program Manager as listed in reference (b).

p. USNA Personnel (employees, contractors, and volunteers). USNA personnel are responsible for safeguarding the rights of others by adhering to the standards set forth in enclosure (3) and references (a) and (b). In addition to the specific responsibilities set forth in paragraph 7 of enclosure (3) to reference (b), USNA personnel will:
(1) Report any loss or breach or suspected loss or breach of PII upon discovery using DD Form 2959 Breach of Personally Identifiable Information (PII) Report.

(2) Mark all records containing PII (e.g. letters, emails, message traffic, etc.) controlled unclassified information (CUI) in accordance with reference (j) and enclosure (3).

(3) Unless approved by the PAC or USNA legal and authorized pursuant to reference (a) section b(3)-b(12), do not disclose any records contained in a system of records maintained by USNA without the written consent of the individual whom the record pertains or pursuant to an “official need to know” within the agency. When disclosing records:

(a) An “official need to know” is that of a demonstrated need for access to the information in the performance of their official duties. The Department of Defense (DoD) is USNA’s agency for this purpose,

(b) Written consent must meet the requirements set forth in enclosure (3) paragraph 6(a)(1), or

(c) If releasing information pursuant to authorization from the PAC or legal pursuant to reference (a) sections b(3)-b(12), individuals must make a log of disclosure pursuant to reference (a) section c(1) as required and send a copy to the PAC.

6. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-InformationManagement/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local record custodian or the USNA Records Manager.

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.

8. Forms and Information Management Control

a. SF901 Controlled Unclassified Information (CUI) Coversheet can be found in the GSA Forms Library, https://www.gsa.gov/reference/forms. DD Form 2959 Breach of Personally Identifiable Information (PII) Report can be found and electronically submitted by Common Access Card (CAC) holders via the Defense Privacy Information Management System (DPIMS)

b. SECNAV 5213/1 SSN Reduction Review Form and OPNAV 5239/14 System Authorization Request can be found on Navy Forms Online at https://forms.documentservices.dla.mil/.SECNAV. SECNAV 5213/1 should be turned into the Privacy Act Coordinator at privacy@usna.edu and OPNAV 5239/14 should be turned in to the Information Technology Services Division when completed.

c. All the USNA forms listed below can be found on the USNA official forms website at https://www.usna.edu/AdminSupport/FormsProgram/USNAOfficialFormsList.php. USNA 5211/1 Naval Academy Personally Identifiable Information Spot Check should be sent to the privacy coordinator at privacy@usna.edu. USNA 5211/2 USNA General Privacy Release Authorization and USNA 5211/4 U.S. Naval Academy Privacy Act Request should be sent to privacy@usna.edu or the proper release authority. USNA 1531/9 USNA Official Transcript Request should be returned to the USNA Registrar at webregistrar@usna.edu. USNA 5400/6 Naval Academy Preparatory School Official Transcript Request should be returned to the NAPS Registrar at registrar-group@naps.edu. USNA 1734/02 MDC Authorization for Release of Information should be submitted to MDC.

d. Reports. The reporting requirement contained in enclosure (3) paragraph 3 is required by reference (b) and was assigned report control symbol SECNAV 5213-1. The reporting requirement contained in paragraph 5n is exempt from reporting requirements per DoDM 8910.01-V1, June 30, 2014 enclosure (3) paragraph 1b(7). The reporting requirement contained in paragraphs 5b(8) and 5p(1) and enclosure (3) paragraph 9 is required by DoDM 5400.11, Volume 2, May 6, 2021 in accordance with OMB Memorandum M-17-12.

S. S. BUCK

Releasability and distribution:
This instruction is cleared for public release and is available only via the USNA directives issuances website, https://www.usna.edu/AdminSupport/Inst/index.php.
REFERENCES

(a) 5 U.S.C. §552a
(b) SECNAVINST 5211.5F
(c) SECNAVINST 5720.42G
(d) 5 U.S.C. §552
(e) DoDI 5400.16 of 14 July 2015
(f) DoD Memorandum of 7 Aug 2019 Titled Treatment of Personally Identifiable Information within Information Impact Level 2 Commercial Cloud Services for the Department of Defense
(g) DISA Memo of 15 Aug 2019 Titled DoD Memorandum of Reciprocity for FedRAMP Authorized Moderate Baseline Cloud Services Offerings (CSO) at Impact Level 2 (IL2)
(h) Public Law 107-0347
(i) SECNAVINST 5720.44C
(j) DoDI 5200.48 of 6 March 2020
DEFINITIONS

1. **Access.** An individual’s ability or opportunity to gain knowledge of Personally Identifiable Information (PII).

2. **Data Owner.** An individual or a group of individuals with responsibility for making decisions regarding the access or granting of access to PII stored in electronic collections (shared drives, MIDS, NSTAR, AIS...).

3. **Disclosure.** The information sharing or transfer of any PII from a system of records 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.

4. **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. Because there are many different types of information that can be used to distinguish or trace an individual’s identity, the term PII is necessarily broad.

5. **PII Breach.** 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, whether physical or electronic.

6. **Privacy Act Complaint.** A complaint received that alleges that an individual has violated another individual’s Privacy Act protected rights. A Privacy Act Complaint could result in a privacy breach upon further investigation.

7. **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 system of records.

8. **Privacy Act Statement (PAS).** A statement containing the authority to collect information, principal purpose of the collection or information, routine uses for the information collected, and whether it is mandatory for an individual to provide their information for a collection of information.

9. **Privacy Impact Assessment (PIA).** A written analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, and determines the risks and effects of maintaining PII in an information technology (IT) system registered in Department of Defense Information Technology Portfolio Registry-DON (DITPRDON). It also examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

10. **Public-Facing Website.** A website containing a collection of information which is freely accessible by all internet users including members of the public.
11. **PA Protected Records.** Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic), about an individual that is maintained by a DoD Component. Information may include, but is not limited to an individual’s education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.

12. **System of Records.** A group of records in which the data about the individual is retrieved by a personal identifier (e.g. name, SSN, date of birth, biometric number, alpha, candidate number, etc.)

13. **System of Records Notice (SORN).** A formal notice published in the Federal Register that constitutes official notification to the public of the existence of a SOR. The notice clearly states what data may be collected and how it will be used, stored, and safeguarded.

See reference (b) for additional definitions relating to the Navy Privacy Program.
USNA PRIVACY PROGRAM REQUIREMENTS AND PROCEDURES

1. Personally Identifiable Information (PII). PII will be handled per references (a) and (b) and the following:

   a. Guides and information for the handling of PII specific to USNA will be promulgated by the USNA Privacy Office and ITSD and posted to the USNA privacy web site at https://www.usna.edu/AdminSupport/Privacy/index.php and/or ITSDs website at https://intrnet.usna.edu/ITSC/policies/index.php. These guides must be adhered to.

   b. Safeguarding PII. In accordance with the minimum standards of safeguarding PII set forth in reference (a) and (b), USNA personnel will:

      (1) Mark all records (email, letters, faxes, excel spreadsheets, forms, etc.) containing PII with the following Controlled Unclassified Information (CUI) markings: CUI on the top and bottom of the record and a CUI designation indicator block (must be included on the first page or cover of the record in the bottom right corner.) Routing folders containing PII should either contain an SF901 CUI Coversheet or contain CUI sticker labels on the top and bottom of the folder, a label at the top right corner indicating the contents of the folder, and a label at the bottom right corner containing the CUI indicator block. PII must not be affixed to the outside of a routing folder. An example of a USNA specific CUI indicator block for PII is included below:

         Controlled by: DON
         Controlled by: USNA (list specific USNA Office such as USNA Admissions)
         CUI Categories: PRVCY (list all privacy categories that apply*)
         Distribution/Dissemination Controls: FEDCON (list appropriate distribution controls**)
         POC: Office phone number or office email responsible for the CUI

*For a listing of CUI categories, see the DoD CUI registry at https://www.dodcui.mil/Home/DoD-CUI-Registry/
**For a listing of dissemination controls, see reference (j)

(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 to be marked as CUI.

(b) Never mark the outer envelopes or any shipping containers as CUI, 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 CUI.

(2) Emails. Emails containing only business related PII do not require CUI markings. For example, sender’s signature blocks (generally containing: name, title, office, business telephone, and email address) do not require CUI markings. Personal email addresses and phone
numbers in list form, when listed as an attachment or listed in the body of an email (like recall rosters), require CUI markings, but personal email addresses in the to/from fields of the email do not require CUI markings when sent to personnel with a need for the content of the email in conducting business and not being used for commercial or personal reasons. When an email requires marking:

(a) Label the subject line as “CUI”.

(b) Label the header and footer of the email body with “CUI”.

(c) Add a CUI “Designation Indicator Block” to the bottom of the email body (within the header and footer) in accordance with reference (j).

(d) Encrypt and digitally sign all emails containing PII, except as noted in paragraph 1.b.(2) above.

(e) Mark attachments containing CUI per the same standards as the body of the email including labeling the attachment as “CUI” in its name. If only the attachment contains PII and the body of the email does not, only the subject of the email and the attachment needs to be labeled with the CUI markings.

(3) Facsimile (fax). USNA personnel may only use fax to transmit PII when absolutely necessary (when a non-DON process requires it, when another more secure means in not practical, or when required by operational necessity). If faxing PII, use a SF901 as a cover sheet and verify receipt by the correct recipient.

(4) PII Data at Rest. The following provisions pertain to PII stored in electronic form. When PII storage is required it must comply with the following restrictions:

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

(b) PII must not be stored on removable electronic media such as a flash drive or external hard drive unless the device is encrypted, marked properly, 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. When a copy of existing PII must be created, the creator is the data owner and is entirely responsible for its protection and markings.

(d) The PII data owner is responsible for ensuring that access to stored PII is restricted to individuals having an “official need to know.”
(e) All files containing PII must include CUI markings per reference (j).

(f) The USNA network file share storage system (network shared drive) is authorized for storing PII. Note: the network file share is neither a user workstation local disk nor a server disk.

(g) PII may be stored on a workstation local disk only if configured as follows:

1. Enterprise-managed full disk encryption that is approved by the USNA Configuration Control Board is configured on the workstation.

2. The end user must not use administrative rights on the workstation to remove encryption.

(h) PII is authorized to be stored utilizing clouds services as authorized by the USNA Configuration Control Board. The USNA Enterprise Collaboration Suite (Drive, Mail, Sheets…) has been approved for the storage of limited PII as approved by the Deputy for Information Technology.

(i) Each use case that requires exposing PII through a web page not explicitly approved in reference (i) must be approved by the USNA Configuration Control Board.

(5) USNA Publicly Accessible Websites. PII should not be posted on a USNA Public-Facing Website with the following exceptions:

(a) The only personnel lists, phone rosters, or organizational charts utilizing names of individuals that are authorized to be posted on USNA Public-Facing Websites are those for senior leadership and, pursuant to reference (i) chapter 7 section 0701 paragraph 3d(2)(c), the USNA 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.

1. Support staff and other departments may list contact information on a Public-Facing Website as long as it is generic (e.g. the Admissions Office main phone number and admissions@usna.edu with no personal identifiers).

2. For the purpose of paragraph 1.b.(5)(a) senior leadership at USNA is defined as the Senior Leadership Team (SLT) members, cost center heads and their deputies, provosts, deans, deputy deans, 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 in paragraph 1.b.(5)(a)2 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 and tracking is required when mailing 25 or more hard copy records containing PII. The inside container must be marked as CUI and contain an SF901. Never mark the outside container as CUI or PII.

(c) Yard mail may be used to send PII as long as an inner envelope is used that is addressed to the recipient, sealed, and marked as CUI and the inner envelope contains an SF901.

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

(a) Shredders must be crosscut and render particles beyond reconstruction. Recommended shred size is 1 mm by 5 mm for PII. The use of a shredder service is authorized according to the following:

1. The service is General Service Approved (GSA).

2. A certificate of destruction is issued and maintained 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. System of Records. 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 number, SSN etc.), it does not qualify as a system of records. System of Records frequently used by USNA personnel are listed on the USNA privacy program website at https://www.usna.edu/AdminSupport/Privacy/index.php.

a. All information collected that will be able to be retrieved by a personal identifier must be governed by a System of Records Notice (SORN); if none exists or one needs to be altered, contact the USNA Privacy Act Coordinator to establish or amend a SORN.
b. USNA personnel must collect, maintain, and retain information in accordance with the SORNs for all the systems of records used or maintained at USNA. Links to all Government wide and DoD SORNs as well as SORN resources can be found on the Defense Privacy, Civil Liberties, and Transparency Division’s website at https://dpcl.ddefense.gov/Privacy/SORNs/.

3. SSN Reduction. In accordance with Department of the Navy SSN Reduction Plan, the following will be adhered to concerning the collection and use of the SSN:

   a. SSN’s must not be requested in surveys or questionnaires, nor included in personnel rosters.

   b. SSNs must not be used in the subject lines of messages, memorandums, letters, or emails nor in the file names of electronic files or folders.

   c. SSNs will only be collected if absolutely necessary and must be authorized per one of the acceptable uses contained in DoDI 1000.30 and approved by the Superintendent or Chief of Staff via SECNAV 5213/1. SECNAV 5213/1 will be maintained by the Privacy Act Coordinator and updated every three years.

4. Privacy Act Statements (PAS). A PAS must be 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. When a PAS is required on a form, it should appear at the top of the form directly under the title or be provided on a separate document (exceptions to this are made on a cases by case basis by the USNA Forms Manager), and will consist of the following elements:

      (1) Authority: This section lists the authority (whether granted by statute, or executive order of the President) which authorizes the solicitation of the information. This section should match the authority section of the governing SORN. The last authority should be a link to the SORN governing the collection of the information. (Note: E.O. 9397 (SSN) must be cited if collecting the 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. This should list the specific routine uses listed in the SORN that pertain to the collection.
(4) Disclosure: State whether providing the information is voluntary or mandatory and the possible effects on the individual if the requested information or part of 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 respondent before any information can be collected for inclusion in a system of records.

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.

5. Privacy Act Advisory (PAA). A PAA is required when collecting information that includes the SSN, and the data will not be stored in a system of records (i.e. not be retrievable by a personal identifier). When required, a privacy advisory will be made up of the following:

a. Authority: List the specific authority for the use of the SSN and E.O. 9397 (SSN), as amended.

b. Disclosure of your SSN is voluntary: List the consequences for not providing the SSN. (i.e. However, if you fail to provide your SSN, we will be unable to grant you access to your records.)

c. Uses to be made of your SSN: Your SSN will be used for identification purposes only. It will not be shared with anyone outside the DoD. Once we have confirmed your identity, we will destroy this form and your information will not become part of any Privacy Act System of Records.

6. Privacy Impact Assessment (PIA). There must be an approved PIA completed in accordance with reference (e) for all USNA information technology and electronic collections that collect, maintain, use, or disseminate PII or those supported through USNA contracts with external sources that collect, maintain, use, or disseminate PII.

7. Privacy Act Requests

a. Processing a first party Privacy Act request or a third-party request with consent of the individual to which the record pertains.

(1) In order for a Privacy Act request to be valid, the following must be met:
(a) The request is in writing. The request, or release if a third party request, must contain the subject of the records full name, complete U.S. postal service mailing address, phone number, and either be:

1. Notarized,

2. Submitted via an official release that includes an unsworn declaration such as USNA 5211/2 USNA Authorization for Disclosure of Information, USNA 1531/9 USNA Official Transcript Request, Naval Academy Preparatory School Official Transcript Request, or USNA 1734/02 MDC Authorization for Release, or

3. Submitted with a signed and dated unsworn declaration stating one of the following:

   a. If executed without the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)”.

   b. If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)”.

(b) The signature required in paragraph 7.a.(1) must be a physical (wet) signature or a digital signature approved per SECNAVINST 5239.24 such as the DoD PKI or DoD-approved PKI.

(c) Only an IDA can deny a Privacy Act request in full or in part. All requests that contain exempt material per reference (a) and cannot be released in full, should be forwarded/referred to the PAC for processing.

(d) If a third-party request for records maintained in a system of records is received without the written consent of the individual to which the record pertains, it should be immediately forwarded to the PAC for release determination under the FOIA unless authorized per reference (a) and approved by legal or the PAC.

(e) Individuals releasing records pursuant to a valid request must ensure the request is tracked and retrievable by name, year request filed, serial number of response letter, or tracking number.

(2) Requests for forms to be filled out or certifications to be completed on behalf of USNA regarding conduct, honor, aptitude, or disciplinary and administrative actions/history should be forwarded to the legal office (e.g. requests to fill out paperwork in regards to applications for law school, the Bar, or employment).
b. Making a USNA Privacy Act Request

(1) USNA must not process requests for records maintained in systems of records under reference (a) unless the requirements of paragraph 7a(1) are met. Requests not meeting these requirements will be processed in accordance with references (c) and (d).

(2) Privacy Act Requests can be submitted in writing directly to the office maintaining the record.

(3) Request for official transcripts or attendance verification should be submitted directly to the registrar’s office. Directions for submitting a request can be found on the USNA Registrar’s website at https://www.usna.edu/Registrar/Transcripts.php or the NAPS Registrar’s website at https://www.usna.edu/NAPS/Registrar.php.

(4) If it is unclear what office maintains the record in question, requests should be submitted directly to the USNA PAC. Directions on submitting a request can be found on the USNA Privacy Program website at https://www.usna.edu/AdminSupport/Privacy/index.php.

8. Unauthorized Disclosure. An unauthorized disclosure of PII or records from a system of records will be treated as a breach and handled per paragraph 9 and the Department of the Navy Breach Response Plan.

9. Breach Reporting

a. Actions when a PII Breach occurs:

(1) Upon discovery, take immediate actions to prevent further disclosure of PII. Do not delete the names or contact information of individuals impacted by the breach. This information will be necessary if notifications are required. Do not report the disclosure of business PII (name, work email, work phone…) as it is not considered a breach.

(2) Once mitigation affects are in place, immediately report the breach utilizing the digital version of DD Form 2959 via the Defense Privacy Information Management System (DPIMS) portal (https://dpims.disa.mil/eCasePortal). Inform the USNA PAC of all breach reports submitted that fall under USNA cognizance via email at privacy@usna.edu. Non-portal traditional DD Form 2959s will only be accepted if the portal is not accessible (i.e. non-CAC holders submitting a breach report). Traditional DD Form 2959s should be sent directly to the PAC.

(3) The Privacy Coordinator will take the required actions via the DPIMS portal to ensure the proper processing of the breach.
(4) If breach notifications are required, the department responsible for the breach will generate the notification letters for Chief of Staff signature within 5 days of receiving notice that notifications are required. The letters must be generated, signed, and mailed within 10 days; and the department responsible for the breach will ensure the letters are mailed within this time frame.

(5) Supervisors of the parties responsible for the breach will provide the Privacy Coordinator with what disciplinary and corrective actions were taken as a result of the breach as well as what actions were taken to prevent reoccurrence within 25 days of notification of the breach.

b. Disciplinary actions against individuals causing PII breaches are always dependent upon the facts and the situation related to the mishandling, failure to protect, compromise or suspected compromise of an individual’s PII. These consequences will be determined by the supervisor and be in accordance with the civilian human resources manual or the Uniform Code of Military Justice. The minimum consequence for an individual responsible for a breach at USNA is taking/re-taking the Navy's annual privacy training available via Navy e-Learning or Total Workforce Management System (TWMS).

10. Privacy Act Complaints. All Privacy Act complaints should be sent to the Privacy Act Coordinator for processing per the guidelines set forth on the Navy Chief Information Officer’s official website (https://www.doncio.navy.mil).