PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Academic and Professionally Accredited Enterprise Education Enclave (AEEE)

2. DOD COMPONENT NAME:

Department of the Navy

United States Naval Academy (USNA)

3. PIA APPROVAL DATE:

PENDING

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The USNA AEEE provides all information technology capabilities common to an undergraduate higher education institution. This encompasses typical functions such as student admissions (AIS, BGIS) and student management (NSTAR, MIDS), including candidate applications and sponsor applications. The personal information collected by the system facilitates evaluation of prospective student enrollment applications, subsequent administration of matriculated students, and management of student sponsors.
PII collected are name, other names used, Social Security Number (SSN), DoD ID Number, driver's license, date of birth, place of birth, gender, race/ethnicity, citizenship, legal status, personal telephone number, home telephone number, personal email address, mailing/home address, religious preference, security clearance, mother's middle name, marital status, height and weight, emergency contact, military records, branch of service, rank, spouse information (name), medical information (condition codes and waivers), disability information (type of disability), law enforcement information (police records, school probation periods), education information (high school name and address, classes or courses taken, cumulative grade point average, class rank, type of diploma, year of high school graduation or expected graduation date, and transcripts), and employment information (work history), and company name, company address, alpha code, candidate number.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected to verify, identify, authenticate, and/or data-match for various mission-related and administrative purposes.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Privacy Act Statements are provided for each collection instrument. The disclosure section implies if the collection is mandatory or voluntary. If the collection is voluntary, individuals are not required to provide the requested information. That section also provides possible consequences for not providing the requested information. The collections are posted in the federal register for 60 day comment before approval and revision.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Collection, use, and maintenance of the information provided is governed by the System of Records Notice (SORN) governing each collection. Individuals give consent to all uses authorized under 5 U.S. Code §552a, to include any specific routine uses outlined in each SORN, when the individual decides to apply for admission or participation in Naval Academy programs.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [X] Privacy Advisory [ ] Not Applicable

Individuals are notified by a Privacy Advisory and a Privacy Act Statement for electronic submissions and Privacy Act statements when utilizing paper submissions. Specific privacy act statements are constructed from the governing SORN for each collection. An example can be found below:
Authority: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 6954, Midshipmen: number; 10 U.S.C. 6956, Midshipmen: Nomination and Selection fill Vacancies; 10 U.S.C. 6957, Selection of Persons from Foreign Countries; 10 U.S.C. 6958, Midshipmen: Qualifications for Admission; 10 U. 6962, Midshipmen: Discharge for Unsatisfactory Conduct or Inaptitude; 10 U.S.C. 6963, Midshipmen: Discharge for Deficiency; OPNAVINST 1531. The Naval Academy Information Program (NAIP); USNAINST 1531.46C, Procedures Governing Assignment to the Reserve Naval Academy Information Pr (NAIP); E.O. 9397 (SSN), as amended; DoDI 1322.22, Service Academies, and N01531-1.
Purpose: To establish an audit trail of files which contain information on individuals as they progress from the application stage, through admissions process, to disenrollment or graduation from the Naval Academy and to maintain information on those applying to assist individual with their progression through the Academy.
Routine Uses: Used by the Admissions Office to evaluate potential candidate merit for admission into the Naval Academy.
Disclosure: Voluntary; however, failure to provide the required information may result in a delay or inability to process the applicant's application or allow for the continued enrollment of a Midshipman at the Naval Academy
LINK to SYSTEM OF RECORDS NOTICE: http://dpclo.defense.gov/Privacy/SORNsIndex/DODComponentArticleView/tabid/7489/Article/6420/n01531-1.aspx

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	Office of the Secretary, CNIC, NETC, NPC, OPNAV, NCIS, OJAG, OGC, and others with a need to know
[X] Other DoD Components	Specify.	Other Service Academies, DoD Academic Entities, DMDC and others with a need to know
[X] Other Federal Agencies	Specify.	SORN Specific Entities
[X] State and Local Agencies	Specify.	Congressional Staffs
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Various (e.g. Adjunct Faculty, HRPP, IT etc.). Contracts will be reviewed and revised to ensure all necessary privacy FAR clauses are incorporated.
[X] Other *(e.g., commercial providers, colleges).*	Specify.	Volunteers, Gratuitous Servants, and other SORN Specific Entities not fitting into the above categories

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals
[X] Databases
[X] Existing DoD Information Systems
[X] Commercial Systems
[X] Other Federal Information Systems

PII is directly input to the system from a variety of electronic and manual sources (e.g. DoD Medical Examination Review Board, Educational Testing Service, Secondary/Post-Secondary schools (various), Law Enforcement Agencies (various), Navy Schools Training Command (NSTC), Navy ROTC, Bank of America, etc.). Data is stored in a single enterprise database encompassing the following information systems:

Admissions Information System (AIS),
Blue and Gold Information System (BGIS),
Naval Academy Preparatory School Scholastic Tracking and Accountability System (NSTAR), and
Midshipmen Information System (MIDS).

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

[X] E-mail
[X] Official Form *(Enter Form Number(s) in the box below)*
[X] Face-to-Face Contact
[X] Paper
[X] Fax
[X] Telephone Interview
[X] Information Sharing - System to System
[X] Website/E-Form
[ ] Other *(If Other, enter the information in the box below)*

USNA does not currently have an approved ERM system, so the AEEE houses all USNA's electronic records to include forms. There are

too many forms to list, but the forms currently feeding directly into the system are USNA 1531/3, USNA 1531/12, USNA 1110/92,93, and 95.

k. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier N01531-1 and see notes below

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

SORNs frequently used by USNA can be found in USNAINST 5211.3series located on the USNA Admin Department website at https://www.usna.edu/AdminSupport/Inst/.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-NU-2015-0001-0022

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Records will be maintained per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

Authorities can be found in each SORN governing records located on this system. As an example, SORN N01531-1 Authorities are below:
10 U.S.C. 5013, Secretary of the Navy.
10 U.S.C. 6956, Midshipmen: Nomination and Selection to fill Vacancies.
10 U.S.C. 6957, Selection of Persons from Foreign Countries.
10 U.S.C. 6958, Midshipmen: Qualifications for Admission.
10 U.S.C. 6962, Midshipmen: Discharge for Unsatisfactory Conduct or Inaptitude.
10 U.S.C. 6963, Midshipmen: Discharge for Deficiency.
E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

This information system houses records containing documents covered by several OMB numbers. The two OMB numbers currently assigned to USNA are 0703-0054 USNA Sponsor Program Application Records (expiration 31 August 19) and 0703-0036 USNA Candidate Application (expired, renewal pending).

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

[X] Biometrics	[X] Birth Date	[X] Child Information
[X] Citizenship	[X] Disability Information	[X] DoD ID Number
[X] Driver's License	[X] Education Information	[X] Emergency Contact
[X] Employment Information	[X] Financial Information	[X] Gender/Gender Identification
[X] Home/Cell Phone	[X] Law Enforcement Information	[X] Legal Status
[X] Mailing/Home Address	[X] Marital Status	[X] Medical Information
[X] Military Records	[X] Mother's Middle/Maiden Name	[X] Name(s)
[X] Official Duty Address	[X] Official Duty Telephone Phone	[X] Other ID Number
[X] Passport Information	[X] Personal E-mail Address	[X] Photo
[X] Place of Birth	[X] Position/Title	[X] Protected Health Information (PHI)[1]
[X] Race/Ethnicity	[X] Rank/Grade	[X] Religious Preference
[X] Records	[X] Securily Information	[X] Social Security Number (SSN) *(Full or in any form)*
[X] Work E-mail Address	[X] If Other, enter the information in the box below	

Education Information: includes high school name and address, classes or courses taken, cumulative grade point average, class rank, type of diploma, year of high school graduation or expected graduation date and transcripts.
Disability Information: includes type of disability.
Law Enforcement Information: includes police records, school probation periods.
Marital Status: includes spouse name.
Medical Information: includes height, weight, condition codes and waivers.
Military Records: includes Graduation class, branch of service and rank.
Name(s): includes other name(s) used.
Other ID Number: Candidate number and Alpha Code.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

[X] Yes [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

10-4-18, Chief of Staff for the Superintendent

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Law Enforcement, National Security and Credentialing: Almost every law enforcement application must be able to report and track individuals through the use of the SSN. This includes, but is not limited to, checks of the National Crime Information Center, state criminal histories and Federal Bureau of Investigation records checks.
Security Clearance Investigation or Verification: The initiation, conduct or verification of security clearances requires the use of the SSN. The SSN is the single identifier that links all the aspects of these investigations. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.
Confirmation of Employment Eligibility: Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove that he or she is eligible to work for or with the U.S. government. Any system that deals with employment eligibility must contain the SSN.
Computer Matching: Systems, processes or forms that interact with other government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching or checking information. These applications should be rigorously scrutinized to determine the availability of some other means of conducting these transactions.
Foreign Travel: DoD personnel are often required to travel beyond U.S. borders, which may require official clearance prior to travel. Currently, the SSN is used as the identifier for these purposes.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

All USNA collection instruments requiring the SSN have been reviewed for compliance with the acceptable use policy. Those not meeting an acceptable use have been removed or replaced and SSN memos justifying the continued use of the SSN in the remaining forms have been

identified and are in progress.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

As the collection of SSNs are used to verify employment eligibility, conduct security clearance review/issuance, law enforcement background/security investigations, and to interface with other Federal databases involving pay and benefits; the SSN cannot be eliminated from AEEE at this time.

b. What is the PII confidentiality impact level[2]? ☐ Low ☐ Moderate ☒ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

☐ Cipher Locks	☒ Closed Circuit TV (CCTV)
☐ Combination Locks	☒ Identification Badges
☒ Key Cards	☒ Safes
☒ Security Guards	☐ If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☒ If Other, enter the information in the box below

Mandatory user agreement disclosure completion prior to system access.
Mandatory user education including annual refresher individual recertification.
SSN Reduction Plan compliance.

(3) Technical Controls. *(Check all that apply)*

☐ Biometrics	☒ Common Access Card (CAC)	☐ DoD Public Key Infrastructure Certificates
☒ Encryption of Data at Rest	☒ Encryption of Data in Transit	☐ External Certificate Authority Certificates
☒ Firewall	☒ Intrusion Detection System (IDS)	☒ Least Privilege Access
☒ Role-Based Access Controls	☐ Used Only for Privileged (Elevated Roles)	☒ User Identification and Password
☒ Virtual Private Network (VPN)	☒ If Other, enter the information in the box below	

Shared drive access permission restrictions.
Remote access controls including time-out functions.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Administrative, operational and technical policies, procedures, processes and practices including but not limited to routine and/or as required review of collected data and collection methods; consolidation or elimination of data fields; user education and training; etc.