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:

Naval Education and Training Future Officer and Citizenship User System (NETFOCUS)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

Naval Education and Training Command (NETC)

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.

Naval Education & Training Future Officer and Citizenship User System (NETFOCUS) serves as the authoritative data source for the Naval Reserve Officer Training Corp (NROTC) and the Naval Junior Reserve Officer Training Corp (NJROTC) programs and provides automated support for the management and administrative functions for Naval Service Training Command (NSTC), Great lakes, Officer Development (OD) and Citizenship Development (CD) programs.

Personal information collected: Name, SSN (Full and truncated), citizenship, gender, race/ethnicity, birth date, personal cell telephone number, personal email address, mailing/home address, security clearance, marital status, financial information, military records, education information.

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 initially collected from NROTC and Seaman to Admiral - 21st Century (STA-21) program applicants. Prospective candidates apply via web applications. NROTC candidates apply for the scholarship program via automated web site, where the candidate is issued a user name and a Federal Information Security Management Act (FISMA)-compliant password. STA-21 scholarship candidates are required to have common-access-card (CAC)/PIN. In each instance, the applicant can enter or view only his/her own data.

Non-candidate user access is managed by authorized administrators within NSTC OD and CD departments. Access is role-based and issued on a need-to-know basis. Access controls and privacy safeguards are in-compliance with DON and DoD policy and guidance.

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.

Failure to provide required information would affect the applicant's submission and chance for acceptance.

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.

Once the individual provides their PII, consent is assumed.

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.)*

☐ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

Privacy Advisory:

We will not obtain personally identifying information about you when you visit our site unless you choose to provide such information to us. If you choose to send an email to the site webmaster or submit an on line feedback form, any contact information that you provide will be solely used to respond to your request and not stored. Please do not provide your full social security (SSN) number to anyone and do not send SSNs or other Privacy Act information via email - that is risky and subject to interception and possible fraudulent use.

NETFOCUS Gateway Consent Banner:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

• The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
• At any time, the USG may inspect and seize data stored on this IS.
• Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
• This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
• Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.
Agree or Disagree

For Official Use Only - Privacy Act Protected

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

☒ Within the DoD Component	Specify.	*Officer Personnel Information System (OPINS)--(outbound only) – SSN, Name, DOB, Citizenship, Place of Birth, Legal Residence *Naval Personnel Command (NPC) PERS-4, PERS-802 *United States Naval Academy (USNA) *Fund Administration and Standardized Document Automation System (FASTDATA) Standard Accounting, Budgeting and Reporting System (SABRS) *Navy Exchange Command (NEXCOM)
☒ Other DoD Components	Specify.	Defense Finance and Accounting Service (DFAS)--(Outbound only) – SSN, Name, Account number, RTN, Account type, Marital Status, Number of Dependents, Legal Residence. *Department of Defense Medical Exam Review Board (DoDMERB)--(Inbound and outbound) – SSN, Name, Date of Birth, Physical Status, Medical Reason code. *Defense Mapping Agency (DMA)
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☐ 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.	

[X] Other *(e.g., commercial providers, colleges).* Specify. *College Board SAT/ACT - Standardized Tests for College Admissions

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

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

Individual:
1. NROTC Scholarship Applicants enter the initial data themselves. The majority of applicants are high school seniors or recent high school graduates.
2. STA-21 Program Applicants also provide the same type of information as NROTC Scholarship applicants. The difference is that STA-21 applicants are active duty enlisted personnel.
3. Throughout a NROTC Midshipman's (MIDN) college career, academic and other program performance information such as PFT data is entered by authorized NROTC Unit staff personnel.
4. The initial record for NJROTC Cadet is manually entered by an authorized user, i.e. the Senior Naval Science Instructor (SNSI) in charge of the local NJROTC unit at the the High School.
5. Department of Defense Medical Exam Review Board (DODMERB). DODMERB provides NETFOCUS with qualification information which is loaded into NETFOCUS.
6. United States Naval Academy (USNA) sends NETFOCUS USNA applicant statistics which are loaded into NETFOCUS.

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

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

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 N01131-1, N01533-2, NM01500-2

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.

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-2015-0001-000

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

(3) Retention Instructions.

New Navy Disposition schedule 1000-7 replaces SSIC 1500.1. Permanent Record. Transfer to FRC when no longer required for research or reference. Transfer to NARA when 25 years old. New NARA Schedule is: DAA-NU-2015-0001-0007

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.

SORN N01131-1, Officer Selection and Appointment System (June 14, 2006, 71 FR 34328),
SORN NM01500-2 Department of the Navy Education and Training Records (Novemeber 22, 2010 75FR71083)
SORN N01533-2 Navy Junior Reserve Officer Training Corps Payment Reimbursement System (July 20, 2009, 74 FR 35171)

5 U.S.C. 301, Departmental Regulations, 10 U.S.C. Sections governing authority to appoint officers; 10 U.S.C. 591, 600, 716, 2107, 2122, 5579, 5600; Merchant Marine Act of 1939 (as amended); and E.O.s 9397, 10450, and 11652.

The enactment of Public Law 88-647 and codification in Title 10, U.S.C., Sec. 2031, authorized the military service secretaries to commission Junior reserve Officers' Training Corps (NJROTC) programs. Title 10, U.S.C.. Sec. 2031 is the statutory basis for the NJROTC program.

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.

☒ 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.

0703-0026 EXPIRATION DATE: 12/31/2019 ICR REFERENCE NUMBER: 201611-0703-001

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)*

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

Financial information: account number, RTN, Account Type
Military Information: PRD -- Projection Rotation Date; EAOS -- End of Obligated Service; PFT data -- Pass/Fail status and overall score
Education Information:
ACT scores – Name, Date of Birth, Home of Record, Score, test type, test date
SAT Scores – Name, SSN, Address, Date of Birth, test date, test scores
High School transcripts – Overall GPA

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?

☒ Yes ☐ No

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

Signed by (18 Apr 2017) Robyn W. Baker, CIO/N6, Naval Education and Training Command (NETC)

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

Computer Matching: NETFOCUS uses SSN to uniquely identify NROTC scholarship applicants who have never been, or may never be issued an DoD ID Number. Legacy System: Interface partners may not be able to complete a timely transition from using SSN as a unique person identifier. For those systems, it may be necessary to continue to exchange data based on the SSN, even though an alternate identifier exists in NETFOCUS.

(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".

NETFOCUS interfaces with the Department of Defense Medical Examination Review Board (DoDMERB) to medically qualify selectees. The DoD ID Number is issued to individuals as a result of the DoDMERB medical qualification process. The nightly NETFOCUS-DEERS web service interface acquires and stores the DoD ID Number. This process has allowed a significant reduction of SSN use throughout NETFOCUS to be implemented.

(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

NETFOCUS has completed an effort to reduce SSN usage by utilizing the DoD ID Number as the unique identifier where possible. With that said, until an alternate methodology can be implemented to synchronize U/I's with interfacing DoN and DoD systems, such as Officer Personnel Information System (OPINS) and Defense Joint Military Pay System-Reserve Component (DJMS-RC), NETFOCUS must continue collecting the SSN.

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
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☐ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☐ 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

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

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

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

User accounts are flagged at 30 days of non-use, disabled after 45 days of non-use and deleted after 60 days.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	DITPR ID: 1496
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	242
[ ]	No		

If "No," explain.

DITPR DON ID: 20813

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

[ ]	Authorization to Operate (ATO)	Date Granted:	
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

IATO:
Granted: 2018-02-05
Expires: 2018-05-31

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[X] Yes [ ] No

If "Yes," Enter UII 007-000001247 If unsure, consult the component IT Budget Point of Contact to obtain the UII