

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:

DD 2475 - DoD Educational Loan Repayment Program Annual Application

2. DOD COMPONENT NAME:

Assistant Secretary of Defense - Reserve Affairs

3. PIA APPROVAL DATE:

09/07/21

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
 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
 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.

For the Military Service to pay a portion of a Service Member's student loan(s). The information provided will be reviewed by Military Service personnel record custodians to verify that eligibility requirements are met. The form will be forwarded to the lender that is identified for verification of the loan amount and status. The form is returned to the Service finance office to make the annual payment to the lender.

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)

Verification that Service Member eligibility requirements are met

e. Do individuals have the opportunity to object to the collection of their PII? 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.

Disclosure of the requested information is voluntary

f. Do individuals have the opportunity to consent to the specific uses of their PII? Yes 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.

By signing the form, the Service Member authorizes the release of the financial data by lender/holder to complete entries.

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 ACT STATEMENT

AUTHORITY: 10 U.S.C. 2171, Education Loan Repayment Program: Enlisted Members on Active Duty in Specified Military Specialties; 2173, Education Loan Repayment Program: Commissioned Officers in Specified Health Professions; 16301, Education Loan Repayment Program: Members of Selected Reserve; 16302, Education Loan Repayment Program: Health Professions Officers Serving in Selected Reserve with Wartime Critical Medical Skill Shortages; 16303, Loan Repayment Program: Chaplains Serving in the Selected Reserve, and E.O. 9397, Social Security Number (SSN).

PRINCIPAL PURPOSE(S): In completing this form, you are requesting your Military Service to pay a portion of your student loan(s). The information you provide will be reviewed by Military Service personnel record custodians to verify that you meet eligibility requirements. This form will then be forwarded to the lender that you identify for verification of the loan amount and status. The form is returned to the Service finance office to make the annual payment to your lender. Collected information is covered by the Applicable Military Service System of Records Notice (SORN) for the Official Military Personnel File or Military Records Jacket. These links can be found at: http://dpclo.defense.gov/privacy/SORNs/component/DOD_Component_Notices.html.

ROUTINE USE(S): To the lender (Department of Education, U.S. Public Health Service, or other financial institution) you identify so that the loan amount and status can be verified. The lender returns the completed form to your unit for additional processing. To the Internal Revenue Service for the purpose of reporting taxable income, and to the credit reporting agencies to assist in the recovery of any improper payments made toward delinquent debts owed by a beneficiary or former beneficiary. The DoD Blanket Routine Uses found at http://privacy.defense.gov/blanket_uses.shtml may apply to this collection.

DISCLOSURE: Voluntary. However, if the requested information is not provided, DoD will not be able to verify the loan amount or status and make the annual payment you are requesting. Your Social Security Number (SSN) is used to ensure accuracy of data involving the specified individual applicant. If you do not provide your SSN, processing of your application may be delayed.

OFFICIAL MILITARY PERSONNEL FILES:

Air Force: http://dpclo.defense.gov/privacy/SORNs/component/airforce/F036_AF_PC_C.html

Army: http://dpclo.defense.gov/privacy/SORNs/component/army/A0600-8-104B_AHRC.html

Army National Guard: http://dpclo.defense.gov/privacy/SORNs/component/army/A0600-8-104b_NGB.html

Navy: <http://dpclo.defense.gov/privacy/SORNs/component/navy/N01070-3.html>

Marine Corps: <http://dpclo.defense.gov/privacy/SORNs/component/usmc/M01070-6.html>

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

- | | | |
|--|----------|---|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | <input type="text" value="Services"/> |
| <input type="checkbox"/> Other DoD Components | Specify. | <input type="text"/> |
| <input checked="" type="checkbox"/> Other Federal Agencies | Specify. | <input type="text" value="DHS, US Coast Guard"/> |
| <input type="checkbox"/> State and Local Agencies | Specify. | <input type="text"/> |
| <input type="checkbox"/> 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. | <input type="text"/> |
| <input checked="" type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | <input type="text" value="Financial Lending Institutions"/> |

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

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

- | | |
|---|---|
| <input type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

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.

Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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.

I. 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.

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

(3) Retention Instructions.

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 statute 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.

AUTHORITY: 10 U.S.C. 2171, Education Loan Repayment Program: Enlisted Members on Active Duty in Specified Military Specialties; 2173, Education Loan Repayment Program: Commissioned Officers in Specified Health Professions; 16301, Education Loan Repayment Program: Members of Selected Reserve; 16302, Education Loan Repayment Program: Health Professions Officers Serving in Selected Reserve with Wartime Critical Medical Skill Shortages; 16303, Loan Repayment Program: Chaplains Serving in the Selected Reserve, and E.O. 9397, Social Security Number (SSN).

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.

OMB No. 0704-0152

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)

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

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.

Cindy L. Allard Chief, Defense Privacy, Civil Liberties, and Transparency Division, 25 MAY 18

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

ROUTINE USE(S): To the lender (Department of Education, U.S. Public Health Service, or other financial institution) you identify so that the loan amount and status can be verified. The lender returns the completed form to your unit for additional processing. To the Internal Revenue Service for the purpose of reporting taxable income, and to the credit reporting agencies to assist in the recovery of any improper payments made toward delinquent debts owed by a beneficiary or former beneficiary. The DoD Blanket Routine Uses found at http://privacy.defense.gov/blanket_uses.shtml may apply to this collection.

(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".

Providing the SSN on the form is voluntary.

(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

Providing the SSN on the form is voluntary.

b. What is the PII confidentiality impact level²? Low Moderate High

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

²Guidance 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)*

- | | |
|---|---|
| <input checked="" type="checkbox"/> Cipher Locks | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> 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)*

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

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