

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:

National Defense University (NDU) Enterprise Information System (NEIS)

2. DOD COMPONENT NAME:

National Defense University

3. PIA APPROVAL DATE:

08/24/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

This data is critical to generate official transcripts for students, Program for Accreditation of Joint Education (PAJE) reports, and Middle States accreditation reports. It is also used to facilitate travel and logistics for foreign nationals who attend the university and their families, as well as HR actions for all University personnel military students. A combination of military, civilian, and/or contract personnel access different combinations of this data in several IT systems. The types of personal information include an individual's name, address, date of birth, phone numbers, e-mail addresses, citizenship, race, sex, age, marital status, spouse information, education and academic data, information pertaining to employment, attributes pertaining to US and Foreign military, civilian, and inter-agency personnel records related to student course enrollments and final grades, Social Security Number (SSN), DoD Identification number, passport number, country of origin, disability and limited medical information, student identification number, grade/rank, branch of service or civilian agency, years of Federal service, security clearance granted and date, biographical data (agency/Service, military operations, assignments, Joint Professional Military Education (JPME) Level, degrees granted, gender, disability, Date of Rank (DOR), Basic Active Service Date (BASD), Joint Service experience, command experience), and financial information (account number and routing 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)

The PII collected is used to verify, identify, match records, and authenticate authorized users. The data is used to generate student transcripts and related reports.

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.

Individuals can object in writing, with a memo provided in Appendix A of NDU Governance and Privacy Program Policy and Procedures. Individuals also read the Privacy Act Statement before submitting PII.

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.

Individuals can object in writing. Individuals also read the Privacy Act Statement before they submit PII.

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. 2165, National Defense University; 10 U.S.C. 2163 Degree Granting Authority for National Defense University and E.O. 9397, as amended (SSN).

PURPOSE: The data provided will be used to update your National Defense University (NDU) record. NDU data are used to authenticate and identify NDU personnel and students; track academic enrollment, assignments, progress, and assessments; track personnel records and actions; create academic transcripts and related reports; facilitate award of degrees and credentials; conduct analysis for regional and DoD academic accreditations; and create reports for University leadership to aid in the development of effective curricula, facilitate academic completion requirements.

ROUTINE USES: Data are shared with other Federal/State agencies and contractors for the purpose of communicating educational credentials and accrediting University programs.

DISCLOSURE: Voluntary. However, if data in NDU systems are not up-to-date, your NDU entitlements/privileges and the ability of NDU systems to identify you as an NDU-affiliated person could be delayed or inaccurate. The production of accurate academic transcripts may not be possible. Home addresses will be used for mustering in the event of an officially declared manmade or natural disaster (DoDI 3001.02) and for notification of a Privacy compromise, loss or stolen (breached) personally identifiable information (PII). If addresses are not correct these two requirements will not be performed with accuracy as to your location.

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.

JDIRs, JS DOM, JS JAG Office

- Other DoD Components Specify.

Military Service Branch Admin/Ops Offices/Military Colleges, Universities and Academies, and Military JAG Offices

- Other Federal Agencies Specify.

Non-DoD Federal Agencies, Federal Law Enforcement Agencies, Congress, and Federal Courts
--
- State and Local Agencies Specify.

State and Local Government Agencies, State and Local Courts, State and Local Law Enforcement Agencies, State and Local IG Offices

- 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.

Intellipeak Solutions, & OSC Edge

- Other (e.g., commercial providers, colleges). Specify.

Former Students/Alumni, Public and Private Domestic and Foreign Universities, Colleges, and Academies

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

- Individuals Databases
- Existing DoD Information Systems Commercial Systems
- Other Federal Information Systems

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

- E-mail Official Form (Enter Form Number(s) in the box below)
- Face-to-Face Contact Paper
- Fax Telephone Interview
- Information Sharing - System to System Website/E-Form
- 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 received 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.

The Archivist of the United States approved the Joint Chiefs of Staff Academic Affairs Records schedule on 22 JUN 2020, DAA-0218-2019-0002.

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.

10 U.S.C. 2165, National Defense University; 10 U.S.C. 2163 Degree Granting Authority for National Defense University and E.O. 9397, as amended (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 control number request is pending. NDU is not yet in receipt of the 60 and/or 30 day notice.