



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Department of Defense Postsecondary Education Complaint System

Office of the Assistant Secretary of Defense

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR** Enter DITPR System Identification Number
- Yes, SIPRNET** Enter SIPRNET Identification Number
- No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes**
 - No**
- If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes**
- No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

0704-0501 (Pending renewal)

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

E.O. 13607, Establishing Principles of Excellence for Educational Institutions Serving Service Members, Veterans, Spouses, and Other Family Members; and DoD Instruction 1322.25, Voluntary Education Programs.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

The DoD Postsecondary Education Complaint System (PECS) provides Uniformed Service Members, spouses, and other family members, and members of the U.S. Coast Guard the opportunity to file formal complaints when educational institutions fail to follow the Principles of Excellence outlined in Executive Order 13607 and the DoD Voluntary Education Partnership MOU. The PECS serves as a collaborative environment that permits DoD personnel the ability to track, manage and process submitted complaints in order to meet the requirements of the executive order and the DoD Voluntary Education Partnership MOU and the Department of Defense Instruction 1322.25, which also establishes the need for PECS and instructs the Services on handling PECS complaints. The PECS data may also be used to perform statistical and program analysis.

PII elements collected:

Name, complaint case ID, DoD Identification (DoD ID) number, pay grade, address, street address, city, state, zip code, country, phone number, age range, email address, service affiliation (service member, spouse or family member, veteran), service branch, service status, sponsor information (service status, service branch, and pay grade), type of education benefits used, school name and , school mailing address, level of study, amount of out-of-pocket tuition or government tuition credit paid (academic year), education center name, education center mailing address, complaint description and resolution, name and contact information of person submitting complaint on behalf of a covered individual.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks to the individual associated with the collected PII are unauthorized access to the data or possible misuse of the data as a result of attacks that include computer hackers, disgruntled employees, and state-sponsored information warfare.

Records are maintained on a guarded military installation, in a secure building in a controlled area accessible only to authorized personnel. Physical entry is restricted by the use of cipher locks and passwords and administrative procedures which are changed periodically. The system is designed with access controls, comprehensive intrusion detection, and virus protection. The application is accessed only by users who have authenticated with either DS Logon or Common Access Card (CAC) authentication. Access to any records in the system is further restricted to only CAC authenticated users, based on role privileges, and who requires the data in the performance of official duties and have completed information assurance and privacy training annually. Data is transmitted via Transport Layer Security (TLS) and Secure Sockets Layer (SSL) encryption to protect session information. Encrypted random tokens are implemented to protect against session hijacking attempts. PECS does not store PII in memory blocks. PECS does not store PII data in cookies or temporary files. Cookies are not cached and are deleted at the termination of each session. PECS database connections are established and terminated at the start and end of each database transaction.

Furthermore, to ensure the integrity of privacy data, all application data are tracked and logged. All data accessible to users are audited for modification and are traceable to a specific user and to a specific time.

Physical security for privacy data is provided by PECS' host (eFOIA/INOSC-East infrastructure) at Langley Air Force Base. As an Air Force establishment, strict physical security measures are always followed.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

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

Specify.

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

Yes **No**

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

The individual can choose to not enter their PII; however, no further action will be taken in order to submit a complaint.

(2) If "No," state the reason why individuals cannot object.

j. 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.

Upon accessing the system, the Privacy Act Statement is displayed which provides information to the complaint filer on how his/her information will be used and/or shared should the complaint be submitted. The individual must then take action by either clicking a button in order to proceed into the collection process, or by simply canceling and exiting the system (if they do not consent to sharing their information). Without specific information pertaining to a complaint, the DoD cannot follow up with a school and if the school cannot identify a particular incident it cannot review for corrections if required. Federal enforcement agencies cannot investigate incidents that may have occurred that warrant further investigation without specific information.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 13607, Establishing Principles of Excellence for Educational Institutions Serving Service Members, Veterans, Spouses, and Other Family Members; and DoD Instruction 1322.25, Voluntary Education Programs.

PURPOSE: To provide Uniformed Service Members, spouses, and other family members the opportunity to file formal complaints when educational institutions fail to follow the Principles of Excellence outlined in E.O. 13607 and DoD Instruction 1322.25 DoD Voluntary Education Partnership MOU.

ROUTINE USE(S): To the Federal Trade Commission Consumer Sentinel Network for access by the Departments of Veterans Affairs, Education, Justice, and the Consumer Financial Protection Bureau for compliance with Executive Order 13607 and potential enforcement efforts. Information may be shared with schools listed in a complaint to aid in the resolution of a case. Applicable Routine Use(s) are: Law Enforcement Routine Use, Congressional Inquiries Disclosure Routine Use, Disclosure When Requesting Information Routine Use, Disclosure of Requested Information Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use.

The Privacy Act System of Records Notice is DPR 44 DoD, DoD Postsecondary Education Complaint System (PECS), found at <http://dpcl.dod.mil/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570751/dpr-44-dod.aspx>

DISCLOSURE: Voluntary. However, failure to provide the information requested may result in a delay in processing your complaint or the inability of Federal agencies to address your complaint.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

DRAFT