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:

Department of Defense Postsecondary Education Complaint System

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

Office of the Assistant Secretary of Defense

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
- [ ] Existing DoD Information System
- [x] 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 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.

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 information is collected to facilitate execution of the DoD voluntary education services programs, policy and compliance with Executive Order 13607 to file and resolve formal complaints when institutions fail to follow the Principles of Excellence and the DoD Voluntary Education Partnership MOU that is included in the DoD Instruction 1322.25.

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.

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

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.

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.

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 [ ] Privacy Advisory [ ] Not Applicable

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.

For a complete list of routine uses, please see the Privacy Act System of Records Notice DPR 44 DoD, DoD Postsecondary Education Complaint System (PECS), found at https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Noties/OSDJS-Article-List/.

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.

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.	OASD(READINESS)/FORCE EDUCATION & TRAINING/VOLUNTARY EDUCATION
[X]	Other DoD Components	Specify.	Air Force, Army, Marines, Navy, and My Career Advancement Account (MyCAA)
[X]	Other Federal Agencies	Specify.	US Coast Guard, Federal Trade Commission, Department of Justice, Department of Veteran Affairs, Department of Education, and Consumer Financial Protection Bureau
[ ]	State and Local Agencies	Specify.	
[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.	BAM Technologies, in performance of contract duties. Contract requires baseline IA controls be implemented to ensure PII is safeguarded. Non-disclosures are in place for all BAM employees working the PECS.
[ ]	Other *(e.g., commercial providers, colleges)*.	Specify.	

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

[X] Individuals [ ] Databases

[X] Existing DoD Information Systems [ ] Commercial Systems

[ ] Other Federal Information Systems

Data gathered from the individual submitting a complaint

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
- [x] Information Sharing - System to System
- [x] 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 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 DPR 44 DoD

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-0330-2013-0017

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

(3) Retention Instructions.

Cut off upon resolution of the case. Record is to be transferred via copy of closed cases to the Federal Trade Commission's Consumer Sentinel System. Records retention period: destroy 3 years after cut off

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.

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.

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.

0704-0501 Department of Defense Postsecondary Education Complaint System - expiring November 20, 2020

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	

DoD Postsecondary Complaint Intake Form asks the complainant to provide:
Complaint case ID, DoD Identification (DoD ID) number, pay grade, age range, 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, 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.

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.

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

(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".

(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

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
- [x] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [x] If Other, enter the information in the box below

AWS GovCloud is a FedRamp partner and is certified to IL4 (Impact Level 4) allowing for PII and other sensitive systems to operate. The platform goes through a rigorous security and certification process through AF Cyber Security and DISA.
Physical security for privacy data is provided by PECS host in the AF/A1 VDC IL4 infrastructure. The purpose of an Amazon GovCloud deployment is designed for Air Force assets, Amazon and the contracting company managing this infrastructure employ physical controls compliant with NIST RMF 800-53 revision 4.

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

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

Data is transmitted via Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption.

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

- [ ] Biometrics
- [x] Common Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [x] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [x] Least Privilege Access
- [x] 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

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