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:
DoDEA Online Registration for Students (DORS) via Registration Gateway

2. DOD COMPONENT NAME: Department of Defense Education Activity

3. PIA APPROVAL DATE: 04/12/21

SECTION 1: PII DESCRIPTION/SUMMARY (FOR PUBLIC RELEASE)
a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)
   - From members of the general public
   - From Federal employees
   ✗ From both members of the general public and Federal employees
   - Not Collected (If checked proceed to Section 4)

b. The PII is in a: (Check one.)
   - New DoD Information System
   - Existing DoD Information System
   ✗ Significantly Modified DoD Information System
   - New Electronic Collection
   - Existing Electronic Collection

   Provides online registration for DoDEA families. Transfers relevant information to DoDEA’s student information system (SIS), Aspen.

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.

PII is required to register students properly to include obtaining appropriate information about students' parents/sponsors and emergency contacts.

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 required to register students properly to include obtaining appropriate information about students' parents/sponsors and emergency contacts.

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.

They can object to the collection by refusing to complete the application or some parts of it; however, failure to complete the application and disclose requested information may delay or prevent the enrollment of a student.

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.

See e. above.

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

*The public reporting burden for this collection of information is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

*Authority: 10 USC Section 2164, 20 US Section 921-932. Principal Purpose: To obtain information necessary to enroll students, administer school operations, and protect student health and welfare in DoD operated dependent educational programs. Completed forms
are covered by the DoDEA Dependent Children’s School Program Files SORN located at http://privacy.defense.gov/notices/DODEA26.shtml. Routine use: To federal, state and local government officials to protect health and safety in the event of emergencies. The DoD Blanket Routine Uses found at http://privacy.defense.gov/blanket_uses.shtml also apply to this collection. Disclosure: Voluntary; however, failure to disclose the information collected on this form may delay and/or prevent the enrollment of a child and/or the delivery of educational and emergency services.

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

☑ Within the DoD Component
☐ Other DoD Components (i.e. Army, Navy, Air Force)
☐ Other Federal Agencies (i.e. Veteran’s Affairs, Energy, State)
☐ State and Local Agencies
☐ 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.)
☐ Other (e.g., commercial providers, colleges).

Specify. Users, developers, registrars, school administrators
Specify. 
Specify. 
Specify. 
Specify. 
Specify.

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

☑ Individuals
☐ Existing DoD Information Systems
☐ Other Federal Information Systems
☐ Databases
☐ Commercial Systems

After parents/sponsors enter their children’s information the first time, DORS repopulates that information for subsequent registrations.

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

☐ E-mail
☐ In-Person Contact
☐ Fax
☑ 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
☑ Website/E-Form

All registration forms are within DORS. Some information comes from Aspen back to DORS.

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 DoDEA 26

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpdld.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-0330-2013-0012-0001

DD FORM 2930, JUN 2017 PREVIOUS EDITION IS OBSOLETE. AEM Designer Page 2 of 8
2. If pending, provide the date the SF-115 was submitted to NARA.

3. Retention instructions.

Retention instructions can be found in the OSD RDS, Series 1900, DoD/DoDEA Schools and Institutions Records (https://www.dodea.edu/Offices/ExecutiveServices/RecordsManagement.cfm).

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 PI not collected or maintained in a system of records, the collection or maintenance of the PI 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 PI. (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 PI.
   (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 USC Section 2164, 20 US Section 921-932.

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.

0704-0495.
**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 | Citizenship | Driver's License | Employment Information | Home/Cell Phone | Mailing/Home Address | Military Records | Official Duty Address | Passport Information | Place of Birth | Race/Ethnicity | Records | Work E-mail Address | Birth Date | Disability Information | Education Information | Financial Information | Law Enforcement Information | Marital Status | Mother's Middle/Maiden Name | Official Duty Telephone Phone | Personal E-mail Address | Position/Title | Rank/Grade | Security Information | If Other, enter the information in the box below | Child Information | DoD ID Number | Emergency Contact | Gender/Gender Identification | Legal Status | Medical Information | Name(s) | Other ID Number | Photo | Protected Health Information (PHI) | Religious Preference | Social Security Number (SSN) (Full or in any form) |
|------------|-------------|-----------------|-----------------------|-----------------|---------------------|-------------------|--------------------|---------------------|-----------------|---------------|---------|---------------------|------------|------------------------|--------------------------|------------------------|--------------------------|-------------|------------------------|----------------|--------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|

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 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 Instruction 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?

   - [ ] Yes
   - [ ] No

   If "Yes," provide the unique identifier and when can it be eliminated?

   If "No," explain.

b. What is the PII confidentiality impact level?  

   - [ ] 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 designee.
c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- [ ] Cipher Locks
- [X] 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)*

- [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

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

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

N/A
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?

- [ ] Yes, DITPR
- [ ] Yes, SIPRNET
- [ ] Yes, RMF tool
- [x] No

If "No," explain.

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:

- [x] Authorization to Operate (ATO)  
  Date Granted: 13/29/2018
- [ ] 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.

(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?

- [ ] Yes  
- [x] No

If "Yes," Enter UII ______________________ If unsure, consult the component IT Budget Point of Contact to obtain the UII.

---

Guidance on Risk Management Framework (RMF) tools (e.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfs.osd.mil.

DD FORM 2930, JUN 2017  PREVIOUS EDITION IS OBSOLETE.