PRIVACY IMPACT ASSESSMENT (PIA)

PRESERVING 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 Notification System (DNS)

2. DOD COMPONENT NAME:

Department of Defense Education Activity

3. PIA APPROVAL DATE:

03/11/21

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

☐ 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.

DNS is a Mass Warning Notification (MWN) system to enable timely dissemination of alerts and warnings of hazards and threats that may impact DoDEA's protected population.

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)

Collected information is used to target appropriate recipients and deliver timely notifications of protective actions needed to avoid the hazard.

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.

Users may choose not to disclose PII during student enrollment.

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.

Users may request not to be sent notifications from DNS by notifying the school registrar or local DNS operator.

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

Parents/Guardians receive Privacy Act Statement when registering DoDEA students in DORS.


PRINCIPAL PURPOSE(S): 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 located at http://www.defense.gov/privacy/doea26.shtml.

ROUTINE USE(S): To Federal, State and local government officials to protect health and safety in the event of emergencies. The DoD
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)

- [X] 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

Specify.

| DNS Program Managers, DNS Regional and District Administrators, and School DNS Operators. |
| Specify. |
| Specify. |
| Specify. |

Reliable Government Solutions Inc.'s subcontractor: BlackBerry.

- The Following requirements shall be incorporated into the DoDEA contract that contain personal data under the Privacy Act:
  - System shall be protected by a firewall and an Intrusion Detection System and have outbound server filtering (egress) implemented at the firewall.
  - Two-factor authentication shall be used for anyone who has access to a significant number of Privacy Act data records from the Internet.
  - Record and/or field level access controls shall be implemented.
  - Security audit logging shall be implemented for all Privacy Act data accesses.
  - Log files shall be reviewed daily.
  - All Privacy Act data shall be removed from the system by overwriting the media 3 times with 0s and 1s before disposal or transfer outside of DoDEA.
  - System shall undergo vulnerability scanning quarterly.
  - System shall use at least 128-bit key encryption to transfer data outside the DoDEA firewall.
  - System developers will only have access to Privacy Act data when it is required in the performance of their duties and compensating controls are in place, discussed and monitored.

- [ ] Other (e.g., commercial providers, colleges).

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

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

DoDEA Student Information System (SIS), Fourth Estate Personnel Accountability and Assessment System (FEPAAS), and DMDC.

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

- [X] E-mail
- [X] In-Person Contact
- [ ] Fax
- [X] 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 |

DoDEA Form 600 (Student Registration) - Intermediary collection instrument.
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 26

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

n/a

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.  

GRS 5.3, item 010 (DAA-GRS-2016-0004-0001)

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

3. Retention Instructions.

Temporary. Cut off when superseded or obsolete. Destroy 3 years after cutoff.

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.

   (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.

DoD Instruction 6055.17, DoD EMERGENCY MANAGEMENT (EM) PROGRAM, Section 5.5, Change 3 Effective June 12, 2019; DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters, May 3, 2010

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: 0704-0495
Expiration Date: April 30, 2023
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 |
| ☐ | Citizenship | ☐ | Disability Information |
| ☐ | Driver's License | ☐ | Education Information |
| ☒ | Employment Information | ☒ | Financial Information |
| ☒ | Home/Cell Phone | ☐ | Law Enforcement Information |
| ☐ | Mailing/Home Address | ☐ | Marital Status |
| ☐ | Military Records | ☐ | Mother's Middle/Maiden Name |
| ☒ | Official Duty Address | ☒ | Official Duty Telephone |
| ☒ | Passport Information | ☒ | Personal E-mail Address |
| ☐ | Place of Birth | ☒ | Position/Title |
| ☐ | Race/Ethnicity | ☐ | Rank/Grade |
| ☐ | Records | ☐ | Security Information |
| ☒ | Work E-mail Address | ☐ | 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) |

Student ID number, Student grade level, and Student Bus number(s).

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.

Does not collect SSN.

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

n/a

(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".

n/a

(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 it can be eliminated?

If "No," explain.

☐ Yes  ☒ No

Not required.

b. What is the PII confidentiality impact level?  ☐ Low  ☒ Moderate  ☐ High

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

‡ 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 (SCO) or designee.
c. How will the PII be secured?

(1) Physical Controls. (Check all that apply)
- Cipher Locks
- Combination Locks
- Key Cards
- Security Guards
- Closed Circuit TV (CCTV)
- Identification Badges
- Safes
- If Other, enter the information in the box below

n/a

(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)
- Biometrics
- Encryption of Data at Rest
- Firewall
- Role-Based Access Controls
- Virtual Private Network (VPN)
- Common Access Card (CAC)
- Encryption of Data in Transit
- Intrusion Detection System (IDS)
- Used Only for Privileged (Elevated Roles)
- If Other, enter the information in the box below

- DoD Public Key Infrastructure Certificates
- External Certificate Authority Certificates
- Least Privilege Access
- 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?

Limited role based access to the system. Only HQ program managers and Contractor system owners have access to the entire DoDEA enterprise in DNS. Regional DNS administrators only have access to the enterprises within their assigned region. District administrators only have access to the enterprises within their assigned district. School level operators are only granted access to the users associated with their school.
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
☒ No

If "No," explain.

DITPR System Identification Number
SIPRNET Identification Number
RMF tool Identification Number

b. DoD information systems require assessment and authorization under the DoD Instruction 5110.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

☐ Authorization to Operate (ATO) Date Granted: 
☐ 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.

System does not have an ATO.

(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 Identifier (UII), required by Office of Management and Budget (OMB) Circular A-117

☐ Yes ☒ 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.