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 Education Activity (DoDEA) Serious Incident Reports & Accident Injury Reports Database

2. DOD COMPONENT NAME:	3. PIA APPROVAL DATE:
Department of Defense Education Activity	09/20/18

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

☒ 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

☒ Existing DoD Information System

☐ Significantly Modified DoD Information System

☐ New Electronic Collection

☐ Existing Electronic Collection

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 system maintains information on events deemed serious incidents (misconduct/accidents/breaches in force protection and individual concerns including suicide/suicide ideation and suicide attempts). Maintained information includes Name, Age, School Grade, and Gender of the subject, and where applicable, victim or potential victim.

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)*

This PII is maintained to identify the subject (s) and potential victim (s) of misconduct, individual concerns (suicide/suicide attempts/suicide ideation/self-injurious behavior). The resulting information is used to conduct trend analysis, track repeat offenders or repeated cases of individual concerns, and comply with specific requirements of law enforcement and/or family advocacy programs.

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.

Information maintained is required to assist in matters of misconduct, trend analysis and tracking repeat offenders

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.

PII used on this form is required to obtain specific Gender/Age/ and Grade demographics for trend analysis that will be reviewed to develop mitigations and when needed shape policy. Names are required to identify repeat offenders, or assist law enforcement or family advocacy programs

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

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.	Education Services (suicide/attempts/ideation), DoDEA Director, DoDEA Chief of Staff, DoDEA Communications Officer, DoDEA Investigations and Internal Review/ DoDEA Security Management Division/DoDEA Title IX Coordinator; FOIA Officer
☒	Other DoD Components	Specify.	Assistant Secretary of Defense for Manpower and Reserve Affairs, law enforcement (Military Police, Millitary Investigative Divisions and other Military Family Service Divisions)
☒	Other Federal Agencies	Specify.	Occupational Safety and Health Administration
☐	State and Local Agencies	Specify.	
☐	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.	
☐	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)*

☒ 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)*

DoDEA Form 4705

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 (007-97-02-07-02-6478-00)

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.   1005-15 (N1-330-11-8)

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

(3) Retention Instructions.

Destroy/Delete when 5 years old. Cut off at the end of the school year. Schools and District safety and Security Officer retain for 2 years. Deputy Director's Safety and Security Office retain for 5 years.

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.

Authority to collect this information is with DoDEA general statutory authority (internal housekeeping), specifically: DoDEA 4700.2 "DoDEA Internal Physical Security" and, DoDEA Regulation 5760.01 "Serious Incident Reporting." 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 2164, Department of Defense Domestic Dependent Elementary and Secondary Schools; 20 U.S.C. 921-932, Overseas Defense Dependent's Education; 29 U.S.C. 794, Nondiscrimination under Federal Grants and 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.

☐ 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.

In accordance with DoD Manual 8910.01, Volume 2 "DoD Information Collections Manual: Procedures for DoD Public Information Collections", SIRS does not require OMB approval due to "Public Information Collections Addressed to Nine or Fewer Persons" and/or "during the conduct of a federal criminal investigation or prosecution, or during the disposition of a particular criminal matter."

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	

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.

> SSN is not provided or requested on this form

(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
☒ 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)*

☐ 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?

Combination of Administrative and Technical Controls

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[3]?

☒	Yes, DITPR	DITPR System Identification Number	14575
☐	Yes, SIPRNET	SIPRNET Identification Number	
☐	Yes, RMF tool	RMF tool Identification Number	
☐	No		

If "No," explain.

This system is internal to DoDEA and resides on a closed DoDEA network

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:

☒	Authorization to Operate (ATO)	Date Granted: 6/12/18
☐	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   ☐ No

If "Yes," Enter UII 000100469   If unsure, consult the component IT Budget Point of Contact to obtain the UII

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