PRIVACY IMPACT ASSESSMENT (PIA)

For the

One Call Now
Department of Defense Education Activity (DoDEA)

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**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

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 DoDEA 26

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

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.

DoDEA 26 SORN; Vol 76, FR 24001

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;
DoD Directive 1342.20, Department of Defense Education Activity (DoDEA);
DoD Directive 1020.1, Nondiscrimination on the Basis of Handicap in Programs and Activities Conducted by the Department of Defense;
and E.O. 9397 (SSN), as amended.

The data is originally collected in support of student registration and entered into the ASPEN database.

Pertinent ASPEN data is transferred to ONE CALL NOW so that ONE CALL NOW can provide notification to parents of security and school related issues.

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.

A system to alert parents via electronic or telephonic means on issues related to their dependent's school. Data utilized to make the electronic or telephonic notifications include: Student Name, Sponsor Name, Sponsor e-mail, Sponsor home, work and cell phone, Spouse's name, Spouse's home work and cell phone, Gender of student, Grade level of student

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

Information is relayed to a non- DOD system for dissemination as needed. Transfer is done via secure means (secure FTP). Contractor has safeguards in place. Each One Call Now (OCN) employee is responsible for maintaining the confidentiality of all personal information to which they have access. Background, criminal, and financial checks on every employee are completed. All employees are subject to random drug testing. As a condition of employment, OCN employees are required to sign a confidentiality agreement that binds them to this responsibility-- even after they leave OCN. OCN has comprehensive security controls to protect against the unauthorized use, alteration, duplication, destruction, disclosure, loss or theft of-and unauthorized access to personal information. When personal information (such as name, address, phone number and credit card number) is received, it is stored on secure servers. OCN ensures the physical, organizational and electronic security of personal information through the use of secure locks on filing cabinets and doors, restricted access to information processing and storage areas, limited access to relevant information by authorized employees only, and passwords, PINs, pass keys and the SSL. Certificates are in place to ensure data encryption or scrambling of electronically transmitted information. OCN follows standard internet and database security practices to keep up-to-date with industry changes. Under no circumstances does OCN sell, rent or give lists of clients or their members to others for use.

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. One Call Now contractor. Contractor provides a controlled network with appropriate

encryption and security that prevents third party access and complies with the Privacy Act of 1974.

☐ **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.

PII is collected as part of the information necessary to generate student records. At the time of collection of the data, a parent could object to providing the data. However, once the data is entered in the ASPEN system, certain data is extracted and transferred to the OCN contractor.

(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.

Data is a necessary part of the school records. Once data is collected and entered into the student's records and the ASPEN system, the data necessary to support OCN emergency notifications is extracted from the ASPEN system..

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: 10 USC 2164, 20 USC 921

PRINCIPAL PURPOSE(S): Required for enrollment of dependents into DoDEA Schools. Provides record of student and sponsor demographic data used in the administration of school programs. Provides emergency contact, pertinent medical and other vital information.

ROUTINE USE(S): Data is collected and entered into the automated School Information Management System for use by DoDEA personnel in providing educational and management programs. Release of student information to non-DoDEA personnel is restricted to U.S. Government personnel and other authorized individuals as approved by DoDEA. Sponsor information may be released to other schools, colleges, and prospective employers as part of the individual student record.

DISCLOSURE: Voluntary. Disclosure of the Social Security Number will expedite the registration process.

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.