



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Summer Workshop Application (SWA) Version 5.0

Department of Defense Education Activity - Headquarters

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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.

Authority for maintenance of the system: (Per DoDEA GC)

Department of Defense Directive 1342.20 "Department of Defense Education Activity";
10 U.S.C. 2164, Department of Defense Domestic Dependent Elementary and Secondary Schools;
20 U.S.C. 921-932, Overseas Defense Dependents Education; and E.O.9397(SSN).

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.

The Summer Workshop Application (SWA) is an online registration service that was developed for the Department of Defense Education Activity (DoDEA) staff (Teachers, Assistant Principals / Principals, District /Area Liaisons, District / Area Coordinators and HQ Personnel). This application helps the staff members of all levels to register for the educational workshops and for the approving authority to review all submitted registrations.

Categories of records in the system:

Records consist of : first name, last name, Social Security Number (full SSN needed to accurately track for salary), renewal transportation agreement, name of area, name of district, name of school or organization, grade level, subjects taught, years with DoDEA, contact personal e-mail address, contact person, contact phone number. (Added per B. Terzian)

The SWA serves as a system for summer/recess appointment pay.

Archives of who took what course and when.

Used for the issuance of travel TDY orders by the districts and area offices and HQ.

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

Risk of unauthorized access to and use of the PII collected information.

To address the risk of unauthorized access to and use of the PII collected information, access to the system is password protected and is authenticated thru DoDEA name and password enabled access to the web server.

Privacy Act notification is prompted upon successful login to the system and is likewise evident in the system's various forms and reports (thru headers and/or footers). In addition, appropriate protection is put in place for the handling of SSNs by blacking-out the first seven digits and displaying only the last four digits of the Social Security Number.

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.

SWA HQ POC, System Administrator/Developer, School Principals, District / Area Coordinators and travel budget personnel, Authorized HQ-Human Resources staff (limited access)

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.

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.

Individuals do have the opportunity to object by declining to apply for a workshop. Furnishing the requested personal data is voluntary. If they do not furnish the requested PII they cannot apply for the workshop or get paid.

All PII collected is required to complete registration/application to a summer workshop. Furthermore, the PII collected and combinations of such is used for: (a) System access authentication; (b) Record identification for registration reviewing authority ; (c) Summer /recess appointment pay; (d) Archive of who took what course; (e) Issuance of travel TDY vouchers.

(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.

See above in section 2.i.2.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Privacy Act notification is prompted upon successful login to the system and is likewise evident in the system's various forms and reports (thru headers and/or footers).

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.