



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

DoDEA Directives Portal System (DoDEA DPS)
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.**



**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.

(2) DoD Instruction, 5025.11, DoD Directives Program.

**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.

This system is for the coordinating of DoDEA Issuances and Internal Guidance documents, to include Directives, Administrative Instructions, Regulations, Directive-Type Memorandums, and Policy Memorandums. It allows multiple business units to coordinate their input on DoDEA Issuances before being signed and distributed.

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

This system contains PII in the form of POC information for designated individual(s) who can be contacted with questions regarding Issuances and Internal Guidance documents. This information includes their name and work phone number and work e-mail address.

This system is protected with physical and technical controls. Both identification badges and proximity badges are required to gain access to the server hardware itself. Technical controls include having document coordinators be designated by their supervisors. They are the only ones who have access to this system. Risks are minimized by requiring users to have a valid DoDEA username and password before they can use the system.

**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.

**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.

(2) If "No," state the reason why individuals cannot object.

Individuals who are designated as POCs are directed to make themselves available for contact as part of their duties. Only their names are collected. Individuals' work phone numbers and work e-mail addresses are also collected but are "owned" by the government as part of the individual's employment.

**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.

Individuals who are designated as POCs are directed to make themselves available for contact as part of their duties. Only their names are collected. Individuals' work phone numbers and work e-mail addresses are also collected but are "owned" by the government as part of the individual's employment. Their information is only used for POC information in the Issuance or Internal Guidance documents.

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.

**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.