# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| |
|---|
| Defense Security Assistance Management System (DSAMS) |
| Defense Security Cooperation Agency |

## 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: 437
- ☐ **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** DSCA 05 (pending review)

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** | TBD (pending OMB review for international military students only) |
| **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.

Foreign Assistance and Arms Export Act, Part II, Chapter 5, IMET, Section 548, Records Regarding Foreign Participants and (a) Development and Maintenance of Database; 10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DoD Directive 5105.38-M, DSCA Manual, Chapter 10; DoD Directive 5101.1, DoD Executive Agent; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; DoD Directive 5105.38-M, DSCA Manual; Joint Security Cooperation Education and Training (JSCET) regulation, (AR12-1, SECNAVINST 4950.4B, AFI 16-105).

**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 purpose of DSAMS is to facilitate case development and implementation and management of the Foreign Military Sales and International Military Education and Training (IMET) Programs. Under DSAMS Training Module (DSAMS-TM), personal information is primarily collected to manage the training activities of IMS selected by the US government to attend various security cooperation training through the Department of Defense (DoD) schools and DoD-contracted facilities.

The types of information collected about individuals are as follows:

International Military Student Data: Full names and aliases, gender, citizenship, country of service, country service number, nationality, date and place of birth, marital status, physical descriptions, biographical data, e-mail addresses, work and home addresses, work, fax and personal telephone numbers, military rank, military unit, identification and student control numbers, student code and US grade, clearance information, passport and visa information, flight crew , dependency data (if accompanied), language capabilities, educational and employment history, personal preferences and training activities.

US Personnel and Foreign Nationals: name, military rank, organization, office telephone number and address.

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

The privacy risks associated with the PII are unauthorized access, inaccurate information entered into the system, and unauthorized disclosure of PII.

However, DSCA is using best industry practices and a DIACAP framework to ensure information is not misused outside of the correct context of the system. All DSAMS TM users with access to the data have valid and current background investigations. Further, access to DSAMS TM information is role based. Users of these systems have access to a limited subset of data based on the concept of least privilege/limited access, and write capability, which is limited to specific roles, is tracked. In addition, the individual user will not have access to the data, except through their systems security software inherent to the operating system and application, and all access is controlled by authentication methods to validate the approved users. The information is also maintained in secured information systems which are located in controlled access facilities, guarded 24 hours a day, and seven days a week.

**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. Defense Institute of Security Assistance Management (DISAM) via the Security Assistance Network (SAN)

☐ **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.

Participation in the international military education and training opportunities in the US is voluntary, and individuals may object to the collection of their PII upon request of the information in-country. However, failure to provide the requested information may result in ineligibility of the training program and prevent access to US installation access.

(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.

All participants implicitly consent to the capture and use of their PII at the time of Invitational Travel Order (ITO) creation and/or nomination for participation in specific events.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

**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. | DSAMS provides a privacy notice at the initial log-in screen for authorized users entering PII data collected from individuals into the system. |
|---|---|

**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.**