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:

Defense Security Assistance Management System (DSAMS)

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

September 15, 2020

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
- [x] 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
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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.

The purpose of DSAMS is to facilitate case development and implementation and management of the Foreign Military Sales (FMS) 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:

U.S. Personnel Data: Full name, military rank, organization, office telephone number and address.

Student Data: Full name and alias, gender, citizenship, country of service, country service number, nationality, date and place of birth, marital status, physical descriptions, biographical data, email addresses, work and home addresses, work, fax and personal telephone numbers, military rank, military unit, worksheet and student control numbers, student code and U.S. grade equivalent, clearance information, passport and visa information, flight crew position type, dependency data (if accompanied), language capabilities, educational and employment history, training activities and personal preferences (e.g. dietary needs, religious accommodations, customs and traditions).

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)*

The selected PII is collected to manage student/participant activities, events and courses. In addition, some of the PII is used for identification purposes for access to DoD information and military facilities. Note, access to the PII data is limited to authorized personnel only. The use of a Department of Defense Common Access Card (CAC) is required for authentication and access to the system data.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

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

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

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

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 [X] Privacy Advisory [ ] Not Applicable

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

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] 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.	
[X] 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.	CONTRACTORS: 1) Information Gateways Inc. (IGI), and 2) General Dynamics Information Technology (GDIT) The contracts contain provisions to ensure the confidentiality and security of PII are in place to manage data risks, including language addressing the completion of orientation and annual privacy training for contractor employees. See Privacy Clauses 52.224-1, 52-224-2 and 52-224-3.
[ ] 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)*

[X] 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
- [ ] Face-to-Face Contact
- [ ] Fax
- [x] Information Sharing - System to System
- [x] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [ ] Website/E-Form

PII data collection is primarily done via the SAN vice DSAMS TM. DSAMS TM is available to select users to use as a back up method for entering student data.

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.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier DSCA 06

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. NC1-330-78-004, item 1a

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

(3) Retention Instructions.

Permanent. Cut off and transfer to NARA when no longer required for reference. NC1-330-78-004, item 1a(1)(a).

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.

22 U.S.C. Chapters 32 and Chapter 39; 10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive (DoDD) 5105.65, Defense Security Cooperation Agency (DSCA); DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, Secretary of the Navy Instruction 4950.4B/Air Force Instruction 16-105, Joint Security Cooperation Education and Training; and DSCA Manual 5105.38-M, Security Assistance Management Manual, Chapter 10, International Training.

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.

OMB Control Number: 0704-0555
Title: Security Assistance Network
IC Title: Security Cooperation Training Management System
Expiration Date: 06/30/2022