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:

DISCS Information System Mission (DISM)

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

05/21/2018

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.

DISCS provides professional education, research, and support to advance U.S. foreign policy through security assistance and cooperation. The DISCS Information System Mission (DISM) was established to hold several web applications for the purpose of better management of students through centralized maintenance of data and to reduce redundancy, including the support of the security cooperation community. DISM also allows for more effective management of personnel within DISCS.

The types of personal information collected in DISM are as follows:

DISCS Personnel data including: Full name, DoD Identification Number (DoD ID) number, gender, date of birth, home address, personal cell phone and work numbers, work domain name, work email address, arrival and departure dates, duty hours, emergency name and contact information, position title, funding source, directorate and office names, employment status, academic rank and degree, salary, job series, civilian grade, military Joint Manpower Program rank and number, date of rank, service branch, occupational specialty code and description, military evaluation dates, tour completion date, recall order, DoD billet manning document number, height and weight, arrival date, security clearance type, issue and expiration dates, investigation type and date, IT level, supervisor name, list of DoD annual training requirements, training completion dates and year required, faculty member, function and program type.

DISCS Personnel Travel data including: Traveler's name, government point of contact information, request number, agency directorate, priority and requirement types, purpose of travel, group and class type, order and voucher numbers, voucher check and Military Interdepartmental Purchase Request (MIPR) dates, funding source, source organization, departure and arrival information, travel location cost information, DoD status of travel request, administrative notes and comments.

Student data including: Full name, student and DoD ID Number, gender, date of birth, nationality, organization and mailing addresses, work number, position title, hotel confirmation number, country name, combatant command, student type, area of expertise and duty type, civilian grade, service branch, military rank, diploma, test scores, supervisor name, email address, and work number, course type, registration date, level and status, certificates, student and registrar comments, administrative notes and emergency point of contact information.

Guest Speaker data including: Full name, position title, gender, social security number (SSN), DoD ID Number, home, cell phone, and work numbers, fax number, email and mailing address, employment status, security clearance type, military rank, civilian grade, course information, honorarium, DISAM host name, and funding information.

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 intended use of the information collected is for mission-related and leadership administrative use as specified above. In addition, the PII is collected to manage personnel actions to include the validation and reconciliation of travel orders, including the management of student/participant activities, events and courses, including certain PII that is used for identification purposes for access to DoD information and military installation.

Finally, PII data is also collected for the purpose of verification, identification, and data matching of the Security Cooperation workforce personnel.

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.

Employees implicitly consent to the capture and use of their PII at the time of employment for various personnel actions (e.g., Human Resources, training and travel, etc.) . Upon the collection of personal information, employees are provided appropriate Privacy Act Statements and given an opportunity to object to any collection of PII at that time.

Regarding members of the general public, participation in the international military education and training courses and opportunities at the Defense Institute of Security Cooperation Studies (DISCS) is voluntary, and individuals may object to the collection of their PII upon request of the information. However, failure to provide the requested information may result in ineligibility of the training program opportunities and prevent access to US installation.

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.

Employees and other participants implicitly consent to the capture and use of their PII at the time of employment and participation in specific training program courses and opportunities, respectively.

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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Authority: 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, Security Assistance Management Manual, Chapter 10; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E. O. 9397, SSN, as amended.

Purpose: The primary use of this information is purposes of efficient administration of U.S. and international students, and the effective management of DISCS personnel and guest lecturers.

Routine Use: Contents shall not be disclosed, discussed or shared with individuals unless they have a direct need-to-know in the performance of their official duties. The information is collected in connection with OSD Privacy Act System Notice DSCA-05, Defense Institute of Security Cooperation Studies Information System Mission (DISM).

Disclosure: Providing the personal information is voluntary. However, failure to provide the requested information may result in ineligibility of certain program opportunities and prevent access to US installation.

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.	DSCA Headquarters and Combatant Commands
[X] Other DoD Components	Specify.	DFAS
[ ] Other Federal Agencies	Specify.	

☐ State and Local Agencies — Specify.

☒ 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. Institute for Defense Analysis (IDA) . The contract contains provisions to ensure the confidentiality and security of PII and safeguards are in place to to manage PII in the workplace. Note, FAR Privacy Act clauses have been added to the contract.

☐ 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)*

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

DD Form 2875

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DSCA 05

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. DAA-330-2013-0003

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

(3) Retention Instructions.

Temporary: Cut off annually, destroy when 25 years old.

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.

10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E.O. 9397, (SSN), as amended.

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.

0704-0548 12/31/2018