PRIVACY IMPACT ASSESSMENT (PIA)

For the

DISAM Information System Mission (DISM)
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	16274
☐	**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 06 (Pending)

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 (Pending)

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.

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347; 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); Foreign Assistance and Arms Export Act § 548; Executive Order 9397, as amended by Executive Order 13478.

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.

DISAM provides professional education, research, and support to advance U.S. foreign policy through security assistance and cooperation. The DISAM 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 DISAM.

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

Guest Speaker data: Full name, position title, gender, social security number (SSN), home, cellular 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.

Personnel data: Full name, gender, date of birth, SSN, domain name, email address, arrival and departure dates, home address, home, cellular and work numbers, duty hours, spouse name, position title, OSD number, funding source, directorate and office names, employment status, academic rank and degree, salary, job series, civilian grade, military JMP rank and number, date of rank, service branch, occupational specialty code and description, military evaluation dates, tour completion date, recall order, manning document number, last PFT, height and weight, military replacement name and arrival date, security clearance type, issue and expiration dates, investigation type and date, official and tourist passport numbers and issue and expiration dates, IT level, supervisor name, list of DoD annual training requirements, training completion dates and year required, faculty member, function and program type, and.

Student data: Full name, SSN (last four digits), student and Electronic Data Interchange Personal Identifier (EDIPI) numbers, 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.

Travel data: Traveler's name, government point of contact information, request number, 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, government charge card account numbers and expiration information, EFT information, DoD status of travel request, conflicting items, administrative notes and comments.

(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. However, records are maintained in a controlled facility. Physical entry is restricted by the use of locks, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by centralized access control to include the use of CAC, passwords (which are changed periodically), file permissions, and audit logs.

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. DSCA Headquarters and Combatant Commands

☒ **Other DoD Components.**

Specify. DFAS

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

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. 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.

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 Assistance Management (DISAM) 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.

(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.

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.

(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.

Upon request of PII data, individuals covered by the Privacy Act are provided appropriate Privacy Act Statements.

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.