# 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:**

Security Assistance Network SC GovCloud (SAGC)

**2. DOD COMPONENT NAME:**

Defense Security Cooperation Agency

**3. PIA APPROVAL DATE:**

## 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.**

Security Cooperation Training Management System (SC-TMS):
IMS Data: Name and alias, full face photograph, gender, citizenship, nationality, date and place of birth, physical descriptions, email addresses, work and home addresses, work and home telephone numbers, marital status, military rank and date of rank, branch of military service, identification and control numbers, clearance, passport and visa information, health information, lodging and travel information, emergency contact(s), language capabilities, educational and employment information, academic evaluation, religious affiliation, preferences (i.e., food, entertainment, etc.), activity remarks, and dependency data (if accompanied).

US Personnel (including Foreign Service National) and Foreign Official at Ministry of Defense (MoD): Name, organization, office telephone and fax numbers, point of contact function, and military rank.

Security Cooperation Workforce Development Database (SCWDD): U.S. Personnel Data: Name and alias, work email address and telephone number, DoD Common Access Card (CAC) Electronic Data Interchange Personal Identifier (EDIPI), student identification number, military service, military rank, civilian grade, professional experience, specialized skills, education and training achieved, career field, military employment code, position/billet information, required personnel type, appointment authority and type, supervisory position, organization, unit identification code (UIC), data source of UIC, security cooperation training, experience and education required, source of training required, security cooperation activity category and function, and contract labor hours, status of security cooperation training and international programs security requirements, rotation and report dates, replacement personnel information, other professional certification program information, remarks and comments.

International Affairs Certification Database (IACD):
Student Information - Full name, email address, mailing addresses, telephone and fax numbers, major command and mailing address, name of organization, office symbol/code, job title, job function, grade/rank, job series, military specialty, start date, total months in International Affairs related work, billet information, current certification level, highest education completed, and field of study.

Supervisor information - First and last name, email address, organization, office symbol, work phone and fax number

SAGC account holders: Name, EDIPI, user group number, organization, job title, office code, country/location code, status (e.g., government employee (American citizen), SAGC affiliation-organization, responsibilities, mailing and email addresses, work, DSN and fax numbers.

**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 students attending DoD schools. In addition, some of the PII is used for identification purposes for access to DoD information and military installation. 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 actions such as training. 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 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); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5101.1, DoD Executive Agent; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Joint Security Cooperation Education and Training (JSCET) regulation, (AR12-1, SECNAVINST 4950.4B, AFI 16-105); Foreign Assistance and Arms Export Act § 548.

Purpose: The primary use of this information is to exchange Security Cooperation personnel management, training and budget information between overseas Security Cooperation Offices, Geographical Combatant Commands, Military Departments, Defense Security Cooperation Agency, Defense Finance and Accounting Services, DoD Schoolhouses, Regional Centers, and International Host Nation Organizations.

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 07, Security Assistance Network (SAGC).

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 Defense Security Cooperation University (DSCU) |
| [X] Other DoD Components | Specify. | Security Cooperation Offices, Combatant Commands, Military Departments, Defense Finance and Accounting Services, DoD Schoolhouses, Regional Centers, and International Host Nation Organizations |

| | | |
|---|---|---|
| ☐ 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

Information is obtained from the individual, official representative, or data exchange with the Defense Security Assistance Management System (DSAMS).

**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)*

**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 07

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.

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

(3) Retention Instructions.

Destroy five years after completion of a specific training program, after period covered by account, from last activity or when superseded or obsolete, whichever is sooner.

**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; 22 U.S.C. 39, Arms Export Control Act, Chapters 32 and Chapter 39; DoD Directive (DoDD) 5105.65, Defense Security Cooperation Agency (DSCA); DoDD 5101.1, DoD Executive Agent; 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 (SAMM), 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
Collection Title: Security Assistance Network SC GovCloud (SAGC)
Expiration Date: 06/30/2022