



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Security Assistance Network (SAN)

Defense Security Cooperation Agency (DSCA)

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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

0704-0555

Enter Expiration Date

5/31/2019

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.

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.

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.

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 Database (SCWD): Name, Electronic Data Interchange Personal Identifier (EDIPI), military rank, position number, source and title, funding source, billet category, higher headquarters, current service, organization, country, state, rotate date, minimal training, and level of training.

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

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

(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, DISAM is using best industry practices and a DIACAP framework to ensure information is not misused outside of the correct context of the system. Further, 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.

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 (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 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.

(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.