PRIVACY IMPACT ASSESSMENT (PIA)

For the

Regional Center Persons/Activity Management System (RCPAMS)
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: 14729
- ☐ **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 03

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)," October 31, 2000, Section 5.10; DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002, Section 5.2.7; DoD Directive 5200.41, "Regional Centers for Security Studies," July 30, 2004, Section 3.1; and DoD Directive 5123.03, "DoD Policy and Responsibilities Relating to Security Cooperation," October 2008

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.

The primary purpose of the Regional Center Persons/Activity Management System (RCPAMS) is to improve management of education opportunities in security cooperation as provided by the Department of Defense through the standardization of business processes across the following five Regional Centers for Security Studies: Africa Center for Strategic Studies (ACSS), Asia-Pacific Center for Security Studies (APCSS), Center for Hemispheric Defense Studies (CHDS), and George Marshall European Center for Security Studies (GCMC), and Near-East-South Asia Center for Strategic Studies (NESA), collectively Regional Centers.

Specifically, RCPAMS provides: (1) a solution for Regional Center staff to manage operational, logistical and cost details about people, events, enrollments and organizations; (2) a tool for reporting on all data related to Regional Center events; (3) a platform for sharing common processes, terminology and data elements to facilitate efficient communication between the Regional Centers; (4) a single view of each person with whom any of the Regional Centers have a relationship, representing the current snapshot and historical record of events and biographical information; (5) an interface to other systems with which the Regional Centers must exchange data for the use by other users and organizations; and (6) an enterprise-class Customer Relationship Management platform to manage two-way communication related to events and their participants.

The system has the capability to collect the following personal information: names, full face photographs, gender, citizenship, date and place of birth, physical descriptions, e-mail addresses, work and home addresses, work and home telephone numbers, military rank, identification and control numbers, passport and visa information, health information, lodging and travel information, emergency contact(s), language capabilities, educational and employment history. Although not covered by US privacy provisions, RCPAMS data collection also includes international military students (IMS) participating in training programs at the Regional Centers.

(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. All RCPAMS users with access to the data have valid and current OPM background investigations. In addition, the individual user will not have access to the data, except through their systems security software inherent to the operating system and application, and all access is controlled by authentication methods to validate the approved users. The information is also maintained in secured information systems which are located in controlled access facilities, guarded 24 hours a day, and seven days a week.

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. The Security Assistance Network (SAN) and GlobalNET

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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. Upon the collection of personal information, the Personnel office provides the employee with appropriate Privacy Act Statements and given an opportunity to object to any collection of PII at that time. Regarding U.S. students, participation in military training opportunities and seminars at the Regional Centers is voluntary. However, failure to provide the information may result in ineligibility.

(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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Employees and US students implicitly consent to the capture and use of their PII at the time of employment and enrollment in the training programs. However, students are given an opportunity through a written release form to authorize or restrict the sharing of their contact information to alumni for networking purposes.

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.

The Regional Centers provide a Privacy Act Statements upon any requests for PII data. The statement outlines the legal authority, purpose, routine use for the collection, as well as, whether or not the information is voluntary and the effects of not providing all or any part of the requested information. In addition, RCPAMS provides a privacy notice at the initial log-in screen for authorized users entering PII data collected from individuals into the system.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☒ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☒ Citizenship	☐ Legal Status	☒ Gender
☒ Race/Ethnicity	☒ Birth Date	☒ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal Email Address
☒ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☒ Spouse Information
☒ Marital Status	☐ Biometrics	☒ Child Information
☐ Financial Information	☒ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☒ Employment Information	☐ Military Records
☒ Emergency Contact	☒ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.

passport and visa information, full face photograph, physical descriptions and language capabilities

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

For US citizens, the source of PII collected from the individual and entered into the system by an authorized user.