

## 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 Cooperation Enterprise Solution (SCES) Application

**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.)

- |  |  |
|--|--|
| <input type="checkbox"/> From members of the general public  | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)   |

**b. The PII is in a:** (Check one)

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.**

The SCES program provides improved access and visibility of case execution data across acquisition, logistics, and financial functional areas to improve management of security cooperation programs across the DOD enterprise. Specifically, SCES Application uses the Security Cooperation Internet Protocol (SCIP) for user access and system authorization purposes and collects only the following PII: Employee Name, User Name (Login), Employee and Party Identification Numbers, Direct Responsibilities (i.e., user account control) and Business Email Address.

**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 PII is collected for mission-related use. The data is used for the workflow process within the application.

**e. Do individuals have the opportunity to object to the collection of their PII?**  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.

If the required information is not provided, the potential user will not receive a SCES Application account.

**f. 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.

Information is used for creation of SCES Application account and information collected is used to establish the users functionality in the workflow process.

**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.)

- Privacy Act Statement       Privacy Advisory       Not Applicable

The Privacy Act Statement is on the first page of the modified DD Form 2875 SCIP SAAR which is required to be completed before a SCES user account is created.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)**

- |   |          |                               |
|---|----------|-------------------------------|
| <input checked="" type="checkbox"/> Within the DoD Component  | Specify. | DSCA                          |
| <input checked="" type="checkbox"/> Other DoD Components  | Specify. | DLA, ARMY, NAVY, AIR FORCE    |
| <input checked="" type="checkbox"/> Other Federal Agencies  | Specify. | STATE DEPARTMENT, COAST GUARD |
| <input type="checkbox"/> State and Local Agencies   | Specify. |                               |
| <input checked="" type="checkbox"/> 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. |                               |
| <input type="checkbox"/> 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)**

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Individuals                      | <input type="checkbox"/> Databases          |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems           |   |

SCIP

**j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)**

- |   |   |
|---|---|
| <input type="checkbox"/> E-mail   | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact                                     | <input type="checkbox"/> Paper  |
| <input type="checkbox"/> Fax  | <input type="checkbox"/> Telephone Interview  |
| <input type="checkbox"/> Information Sharing - System to System                   | <input checked="" type="checkbox"/> Website/E-Form  |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) |   |

Modified DD Form 2875 SCIP SAAR

**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

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcid.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.

11/29/2017

(3) Retention Instructions.

**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 statute 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 (DoDD) 5101.1, DoD Executive Agent; DoDD 5105.65, Defense Security Cooperation Agency (DSCA); DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; and DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities

**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.

DSCA's Information Management Control Officer (IMCO) cleared the collection on October 1, 2017. No OMB approval is required. The system receives the user's name and email address from the Security Cooperation Information Portal (SCIP). All other fields on the SCES User form is uneditable and cannot capture any information from the user.