

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:

DISCS Information System Mission (DISM)

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.

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

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

DISCS Personnel data including: Full name, DoD Identification Number (DoD ID) number, gender, date of birth, home address, personal cell phone and work numbers, work domain name, work email address, arrival and departure dates, duty hours, emergency name and contact information, position title, funding source, directorate and office names, employment status, academic rank and degree, salary, job series, civilian grade, military Joint Manpower Program rank and number, date of rank, service branch, occupational specialty code and description, military evaluation dates, tour completion date, recall order, DoD billet manning document number, height and weight, arrival date, security clearance type, issue and expiration dates, investigation type and date, IT level, supervisor name, list of DoD annual training requirements, training completion dates and year required, faculty member, function and program type.

DISCS Personnel Travel data including: Traveler's name, government point of contact information, request number, agency 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, DoD status of travel request, administrative notes and comments.

Student data including: Full name, student and DoD ID Number, 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.

Guest Speaker data including: Full name, position title, gender, social security number (SSN), DoD ID Number, home, cell phone, 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.

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 intended use of the information collected is for mission-related and leadership administrative use as specified above. In addition, the PII is collected to manage personnel actions to include the validation and reconciliation of travel orders, including the management of student/participant activities, events and courses, including certain PII that is used for identification purposes for access to DoD information and military installation.

Finally, 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? 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 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 Cooperation Studies (DISCS) 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? 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.)

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); DoD Directive 5105.38-M, Security Assistance Management Manual, Chapter 10; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E. O. 9397, SSN, as amended.

Purpose: The primary use of this information is purposes of efficient administration of U.S. and international students, and the effective management of DISCS personnel and guest lecturers.

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-05, Defense Institute of Security Cooperation Studies Information System Mission (DISM).

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)

- Within the DoD Component Specify.
- Other DoD Components Specify.
- 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

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)

DD Form 2875

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://dpcl.d.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.

Temporary: Cut off annually, destroy when 25 years old.

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 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E.O. 9397, (SSN), as amended.

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.

0704-0548 12/31/2018

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Birth Date | <input type="checkbox"/> Child Information |
| <input checked="" type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Education Information | <input checked="" type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Gender Identification |
| <input checked="" type="checkbox"/> Home/Cell Phone | <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input checked="" type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone Phone | <input checked="" type="checkbox"/> Other ID Number |
| <input checked="" type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input checked="" type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input checked="" type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input checked="" type="checkbox"/> Records | <input checked="" type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input checked="" type="checkbox"/> Work E-mail Address | <input type="checkbox"/> If Other, enter the information in the box below | |

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

- Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Signed by Lieutenant General Charles W. Hooper, USA on June 29, 2018.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

The collection and continued use of the Social Security Number (SSN) collected within the Defense Institute of Security Cooperation Studies (DISCS) Information System Mission (DISM) for reimbursement of travel expenses and honorarium.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

DISCS is using best industry practices and the DoD Risk Management Framework (RMF) process to ensure the SSN, along with other personal data within DISM, is not misused outside of the correct context of the system. 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 Common Access Cards, passwords (which are changed periodically), file permissions and audit logs.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

- Yes No

The use of EDIPI shall be utilized once the DTS interface has been upgraded to use EDIPI instead of SSN for travel reimbursements.

b. What is the PII confidentiality impact level²? Low Moderate High

¹The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

²Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- | | |
|-------------------------------------------------------|--------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Cipher Locks | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input type="checkbox"/> Identification Badges |
| <input type="checkbox"/> Key Cards | <input type="checkbox"/> Safes |
| <input type="checkbox"/> Security Guards | <input checked="" type="checkbox"/> If Other, enter the information in the box below |

Paper documentation will be stored in locked file cabinets.

(2) Administrative Controls. *(Check all that apply)*

- Backups Secured Off-site
- Encryption of Backups
- Methods to Ensure Only Authorized Personnel Access to PII
- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- | | | |
|----------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Command Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input checked="" type="checkbox"/> Least Privilege Access |
| <input checked="" type="checkbox"/> Role-Based Access Controls | <input type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password |
| <input type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> If Other, enter the information in the box below | |

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

PII data is protected by physical security controls to include locking rooms and cabinets at the end of the day, providing individuals who process PII data with Privacy Act data specialized training, and ensuring the data is encrypted during data transmission. Additionally, data devices leaving the building containing PII are encrypted.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool³?

<input checked="" type="checkbox"/> Yes, DITPR	DITPR System Identification Number	<input type="text" value="16274"/>
<input type="checkbox"/> Yes, SIPRNET	SIPRNET Identification Number	<input type="text"/>
<input checked="" type="checkbox"/> Yes, RMF tool	RMF tool Identification Number	<input type="text" value="5"/>
<input type="checkbox"/> No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

<input checked="" type="checkbox"/> Authorization to Operate (ATO)	Date Granted:	<input type="text" value="11/22/2017"/>
<input type="checkbox"/> ATO with Conditions	Date Granted:	<input type="text"/>
<input type="checkbox"/> Denial of Authorization to Operate (DATO)	Date Granted:	<input type="text"/>
<input type="checkbox"/> Interim Authorization to Test (IATT)	Date Granted:	<input type="text"/>

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

Yes No

If "Yes," Enter UII If unsure, consult the component IT Budget Point of Contact to obtain the UII

³Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at <https://rmfks.osd.mil>.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Dwayne L. Eldridge	(1) Title	Director of Academic Planning and Technology	
	(2) Organization	Defense Institute Security Cooperation Studies	(3) Work Telephone	(937) 713-3307
	(4) DSN	(312) 713-3307	(5) E-mail address	dwayne.l.eldridge.civ@mail.mil
	(6) Date of Review		(7) Signature	
b. Other Official (to be used at Component discretion)	Mark T. Ahles	(1) Title	Deputy Commandant	
	(2) Organization	Defense Institute Security Cooperation Studies	(3) Work Telephone	(937) 713-3303
	(4) DSN	(312) 713-3303	(5) E-mail address	mark.t.ahles.civ@mail.mil
	(6) Date of Review	05/21/18	(7) Signature	
c. Other Official (to be used at Component discretion)		(1) Title		
	(2) Organization		(3) Work Telephone	
	(4) DSN		(5) E-mail address	
	(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Teresa D. Simpson	(1) Title	FOIA/Privacy Act Officer	
	(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(703) 697-9032
	(4) DSN		(5) E-mail address	teresa.d.simpson.civ@mail.mil
	(6) Date of Review		(7) Signature	

e. Component Records Officer	Richard Williamson	(1) Title	Branch Chief
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(703) 697-1965
(4) DSN	UNK	(5) E-mail address	richard.c.williamson14.civ@mail.mil
(6) Date of Review	06/01/18	(7) Signature	
f. Component Senior Information Security Officer or Designee Name	Ronald Greenfield	(1) Title	Chief, Cybersecurity
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(703) 697-9609
(4) DSN		(5) E-mail address	ronald.l.greenfield.civ@mail.mil
(6) Date of Review:		(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name	Roger B. Sabin	(1) Title	General Counsel
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(703) 697-9024
(4) DSN		(5) E-mail address	roger.b.sabin.civ@mail.mil
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name	Lisa Jollay	(1) Title	Chief Information Officer
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(703) 697-9769
(4) DSN		(5) E-mail address	lisa.l.jollay.civ@mail.mil
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.