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:

Case Launcher

2. DOD COMPONENT NAME:

Defense Security Cooperation Agency

3. PIA APPROVAL DATE:

05/18/26

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] 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.

The Case Launcher replaces for Defense Security Assistance Management System (DSAMS) used for the development and implementation of all unclassified cases for Foreign Military Sales (FMS), International Military Education and Training (IMET), and other aspects of Security Cooperation and Security Assistance involving the transfer of defense material, services or training, via sale, grant or lease, to allied and friendly foreign countries and international organizations under the authority of the Arms Export Control Act, the Foreign Assistance Act, and other laws and regulations. See Section 2 for specific PII collected.

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 use is for authentication, access and audit purposes.

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.

Prior to the collection of PII, users are provided appropriate Privacy Act Statement via DD Form 2875 and given an opportunity to object to any collection of PII at that time. However, if the requested information is not provided, the potential user will not receive access to the system.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

Users implicitly consent to the capture and specific use of their Pll upon completion of DD Form 2875 for account creation and access. However, if the requested information is not provided, the potential user will not receive access to the system.

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

Upon the collection of PII, individuals subject to the Privacy Act are provided appropriate Privacy Act Statements. For access, DD Form 2875, System Authorization Access Request (SAAR) is completed, and the form includes the following Privacy Act Statement:

Authority: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

Purpose: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

Routine Use: None.

Disclosure: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

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

☒ Within the DoD Component	Specify.	Interfaces with Security Cooperation Enterprise System (SCES), Security Assistance Network (SAN) and 1200 System
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Legacy DSAMS Database
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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.	CONTRACTOR(S): Deloitte & Touche LLP The contracts contain provisions to ensure the confidentiality and security of PII are in place to manage data risks, including language addressing the completion of orientation and annual privacy training for contractor employees. See Privacy Clauses 52.224-1, 52-224-2 and 52-224-3.
☐ 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)*

☐ In-Person 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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DoD 0019

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. NC1-330-78-004, item 1a(1)(a)

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

(3) Retention Instructions.

File Number: 810-102.1 Foreign Military Sales (FMS) (DSCA) (AR)1100 Master File
Disposition Instructions: Permanent. Cut off and transfer to NARA when no longer required for reference.

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.

22 U.S.C. Chapters 32 and Chapter 39; 10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive (DoDD) 5105.65, Defense Security Cooperation Agency (DSCA); 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, 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 [X] 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.

The collection is exempted from OMB approval because it uses only a minimal identifier primarily for access purposes.

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)*

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

User ID

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 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.

Not Applicable

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

Not Applicable

(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".

Not Applicable

(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

Not Applicable - no SSN collected.

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

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

[2]Guidance 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)*

- [ ] Cipher Locks
- [ ] Combination Locks
- [x] Key Cards
- [x] Security Guards
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

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

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

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

- [ ] Biometrics
- [ ] Encryption of Data at Rest
- [ ] Firewall
- [x] Role-Based Access Controls
- [ ] Virtual Private Network (VPN)
- [x] Common Access Card (CAC)
- [x] Encryption of Data in Transit
- [ ] Intrusion Detection System (IDS)
- [ ] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [ ] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [ ] Least Privilege Access
- [ ] User Identification and Password

Case Laucher is hosted on AWS GovCloud in the EC3S environment and will inherit controls from EC3S and AWS. Additionally, the system will use the DISA Citadel DevSecOps pipeline and will inherit some controls from Citadel as well.

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

DSCA has instituted safeguards at each stage of the information cycle by protecting individual privacy in accordance with best industry practices.

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) tool[3]?

☐	Yes, DITPR	DITPR System Identification Number	
☐	Yes, SIPRNET	SIPRNET Identification Number	
☒	Yes, RMF tool	RMF tool Identification Number	104
☐	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:

☐	Authorization to Operate (ATO)	Date Granted:	
☐	ATO with Conditions	Date Granted:	
☐	Denial of Authorization to Operate (DATO)	Date Granted:	
☐	Interim Authorization to Test (IATT)	Date Granted:	

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

System not yet assessed. Projected date of completion 29 September 2026

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

N/A

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.

[3]Guidance on Risk Management Framework (RMF) tools (i.e., 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	Andrew Brown	(1) Title	Program Manager
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(223) 758-3254
(4) DSN		(5) E-mail address	andrew.t.brown40.civ@mail.mil
(6) Signature	BROWN.ANDREW.T.1283532468 Digitally signed by BROWN.ANDREW.T.1283532468 Date: 2026.03.16 09:46:55 -04'00'	(7) Date of Review	03/16/26
b. Other Official ***(to be used at Component discretion)***	Steven Smith	(1) Title	ISSO
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	
(4) DSN		(5) E-mail address	steven.j.smith365.ctr@mail.mil
(6) Signature	SMITH.STEVEN.JAMES.1514600933 Digitally signed by SMITH.STEVEN.JAMES.1514600933 Date: 2026.03.16 08:49:19 -05'00'	(7) Date of Review	03/16/26
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Signature		(7) Date of Review	
d. Component Privacy Officer (CPO)	Teresa D. Simpson	(1) Title	Government Information Specialist
(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) Signature		(7) Date of Review	

e. Component Records Officer	Jeffrey Troch	(1) Title	Chief, Knowledge Management and Records Designee
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(223) 758-3336
(4) DSN		(5) E-mail address	jeffrey.l.troch.civ@mail.mil
(6) Signature	TROCH.JEFFREY.LEE.1035114544 Digitally signed by TROCH.JEFFREY.LEE.1035114544 Date: 2026.03.20 11:49:57 -04'00'	(7) Date of Review	03/20/26
f. Component Senior Information Security Officer or Designee Name	Josh Dill	(1) Title	Chief Information Security Officer
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	(223) 758-3453
(4) DSN		(5) E-mail address	joshua.dill2.civ@mail.mil
(6) Signature	DILL.JOSHUA.1383141849 Digitally signed by DILL.JOSHUA.1383141849 Date: 2026.03.16 10:02:32 -04'00'	(7) Date of Review	
g. Senior Component Official for Privacy (SCOP) or Designee Name	Tameka M. Collier	(1) Title	Senior Component Official for Privacy
(2) Organization	Defense Security Cooperation Agency	(3) Work Telephone	703-697-9024
(4) DSN		(5) E-mail address	tameka.m.collier.civ@mail.mil
(6) Signature	COLLIER.TAMEKA.M.1456348285 Digitally signed by COLLIER.TAMEKA.M.1456348285 Date: 2026.05.15 13:23:09 -04'00'	(7) Date of Review	
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) Signature	JOLLAY.LISA.L.1134012745 Digitally signed by JOLLAY.LISA.L.1134012745 Date: 2026.05.18 10:34:44 -04'00'	(7) Date of Review	05/18/26

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.