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:

DCSA Enterprise Service Delivery Platform

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

07/18/2025

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
- ☒ 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.)*

- ☐ 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 Enterprise Service Delivery Software as a Service (SaaS) Platform is a FedRamp certified cloud service provider solution that allows primarily Agency Back-Office or Mission Enabling components to automate previously manual processes, such as DCSA internal personnel management, mission-specific case/information/records management, workflow tracking and business operations. The Agency stakeholder solutions utilize the ServiceNow Enterprise Licensing Agreement (ELA) Module Suites of IT Service Management (ITSM), Public Sector Digital Services (PSDS), Strategic Portfolio Management (SPM), Workplace Service Delivery (WSD), Hardware and Software Asset Management, Integrated Risk Management (IRM), and Human Resource Service Delivery (HRSD). ESDP supports various DCSA enabling mission areas (eg. HR, Labor/Employee Relations, Personnel Vetting, Personnel Security, Insider Threat, Inspector General, General Counsel, Cybersecurity, Acquisitions, Billing, Budget, etc.) and the various supporting applications/modules utilized by these missions which may include non-personal, non-PII, PII, and PHI data. Not all modules use or contain sensitive personal or financial information; data collected is application/module-specific and dependent on the mission area and purpose that module serves. See application attachments for additional details.

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)*

PII is collected for verification, validation, identification, authentication, and data matching to support work involving mission operations and functions listed in section 1.c.. As mentioned, not all modules collect, use, or contain sensitive personal or financial information; data collected/used is application/module-specific and dependent on the mission area and purpose that module serves. The use varies based on the collection authorization and needs to fulfill business operations for the respective mission area (eg. HR, Labor/Employee Relations, Personnel Vetting, Personnel Security, Insider Threat, Inspector General, General Counsel, Cybersecurity, Acquisitions, Billing, Budget, etc.) See application attachments for additional details.

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.

Individuals do not have the opportunity to object to the collection of their PII contained within ESD. Users may have the opportunity to object to the collection of their PII through initial information collection, such as an approved Standard (SF) or DD Form, which feeds into ESD applications but they are not able to object DCSA using the collected PII contained within the ESD system itself.

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.

The source of the information collection provides whether the information is voluntary or mandatory; completing of the source information provides the authority and routine uses for the process. ESD is an automation of those processes, however, and individuals are not able to consent to use within the ESD system itself.

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

As described above, PII data collection occurs outside of ESD. The system does contain banners and/or flags to users regarding potential PII and what type of information should or should not be entered into certain fields. Individuals who are asked to provide specific PII on forms are furnished with a Privacy Act Statement and/or Advisory.

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.	DCSA
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	DoD data/system exchanges are based on specific applications and documented separately in a designated PTA and ISA. Data system/exchange includes, but is not limited to, DLA, MILDEPS, and clearance sponsoring organizations.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	DoD data/system exchanges are based on specific applications and documented separately in a designated PTA and ISA. Data system/exchanges includes, but is not limited to, personnel record information.
☐ 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.	KPMG and BAH contracted resources for managing the ESD application baselines. All contractors covered under the National Industrial Security Program (NISP).
☐ 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)*

Official Forms vary based on the mission area and purpose. ESD is a tool for tracking and automation, it may ingest report data that originated from other systems, as determined by mission area, but it does not presently transmit data to other systems.

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 See attached SORN System identifier list

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. See attached NARA list

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

(3) Retention Instructions.

See attached NARA list

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.

The authorities to collect information that may be applicable (See applications attachments for additional details.) are as follows: Executive Orders 10450, 10577, 10865, 12333, and 12968; sections 3301, 3302, and 9101 of title 5, United States Code (U.S.C.); sections 2165 and 2201 of title 42, U.S.C.; chapter 23 of title 50, U.S.C.; and parts 2, 5, 731, 732, and 736 of title 5, Code of Federal Regulations (CFR). In addition, the authority for soliciting and verifying your SSN is Executive Order 9397, as amended by EO 13478. In addition, 5 U.S.C. 552, 5 U.S.C. 552a, 32 CFR 310, and 32 CFR 286 are the authorities to collect information on the INV 100 and DCSA Form 335. 10 U.S.C. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: Qualifications, term, grade; Atomic Energy Act of 1954, 60 Stat. 755; Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 401 note); Public Law 114-92, Section 1086, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Reform and Improvement of Personnel Security, Insider Threat Detection and Prevention, and Physical Security (10 U.S.C. 1564 note); Public Law 114-328, Section 951 (NDAA for FY2017), Enhanced Security Programs for Department Defense Personnel and Innovation Initiatives (10 U.S.C. 1564 note); Public Law 115-91, Section 925, (NDAA for FY2018) Background and Security Investigations for Department of Defense Personnel (10 U.S.C. 1564 note); 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; Executive Order (E.O.) 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities

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.

See Addendum, OMB Control Number list for the information collections within ESDP.