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:

Enterprise Data Governance Center (EDGC)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

03/17/2026

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 Data Governance Center (EDGC) program is designed to enhance data intelligence by establishing a centralized platform for discovering, sharing, cataloging and managing the quality of DCSA's data assets. EDGC utilizes a Collibra server as a business-facing data governance software platform providing data governance, data catalog, workflow, stewardship, dashboards, lineage, policy management, user management, privilege management, and help desk capabilities to enhance and support the DoD & DCSA Data Strategy. EDGC is also comprised of the Integrated Security Data Services (ISDS). The ISDS serves as a data access point federating systems and storage of certain data to enable DCSA missions to reach a single data layer for data. The ISDS will utilize Collibra to define data ownership, establish data quality rules, and manage data lineage, ensuring compliance with agency and DoD data security and governance standards. This integration will extend its governance framework to encompass the data assets and services provided by the ISDS.

Personal information accessible through the platform include data reported on the following forms: Personnel Vetting Questionnaire (PVQ), SF-85: Questionnaire for Non-sensitive Positions, SF-85P: Questionnaire for Public Trust Positions, SF-85P-S: Supplemental Questionnaire for Selected Positions, SF-86: Questionnaire for National Security Positions, Results of Investigation, commercially available information, and publicly available information. The data is collected by existing missions for their expressed purposes. The Integrated Security Data Services (ISDS) capability is a unified data ecosystem allowing data to be leveraged to meet any mission or business need by eliminating critical capability gaps in data delivery which prevent the agency from maximizing the value of integrating and utilizing its data to address critical national security threats and risks. ISDS federates this access to enable missions to share data over a common, controlled, secured interface. PII processed within the ISDS may be subject to data analysis to support customers within the enterprise. An example of PII use may be data studies related to background investigations or SF-86 data.

The system's primary function is the analysis of comprehensive enterprise data, not specifically Personally Identifiable Information (PII). PII is accessed through EDGC through role-based and attribute-based access controls.

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)*

Depending upon the mission need, SSN will be retrieved with other record information if the authorized user or system has the appropriate attributes and privileges to handle sensitive information of that nature. SSNs are used in the forms and in the system as identification of individuals. The ISDS use of SSNs fall under DoD 1000.30 Enclosure 2, section 3: Security Clearance Investigation or Verification.

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.

ISDS does not collect PII directly, but maintains access to data sets that have their own mission traceability. The missions owning the need

for the data control these mechanisms.

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.

ISDS does not collect PII directly, but maintains access to data sets that have their own mission traceability. The missions owning the need for the data control these mechanisms.

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

ISDS itself does not collect Personally Identifiable Information (PII). Instead, it provides access to datasets, each with its own defined mission traceability. The organizations responsible for the missions that require the data retain control over the mechanisms governing access to those datasets.

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.	Internal DCSA: Personnel Vetting, Program Acquisition Executive, Data Office
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ 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.	Booz Allen Hamilton Specific FAR privacy clauses are not directly identified, however the following language is contained within: Article XIV, Section B: Protecting Controlled Unclassified Information in Non-federal Information Systems (page 22): This clause mandates the protection of "covered defense information," which includes PII, and requires adherence to NIST standards. o "The Performer shall Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-" Article XIV, Section B: Protecting Controlled Unclassified Information in Non-federal Information Systems (page 22): This clause mandates the protection of "covered defense information," which includes PII, and requires adherence to NIST standards. o "The Performer shall provide adequate security to safeguard covered defense information that resides on or is transiting through the performer's internal information system or network, as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Non-federal Information Systems."" Article XIV, Section N: Privacy Act of 1974 (page 28): This section explicitly requires compliance with the Privacy Act. o Privacy Act of 1974: "The Performer shall Comply with the Privacy Act of1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-The systems of records; and The

design, development, or operation work that the Performer is to perform;"
o "The Performer shall include the Privacy Act notification contained within this agreement in every sub- agreement when the work statement in the proposed sub-agreement requires the design, development, or operation of a system of records on individuals that is subject to the Act;"

☐ 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
☒ Existing DoD Information Systems
☒ Other Federal Information Systems
☐ Databases
☒ Commercial Systems

Please see Addendum.

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

☐ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☐ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☐ Telephone Interview
☐ Website/E-Form

Existing systems collect PII.

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 Please see Addendum.

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. Please see Addendum.

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

(3) Retention Instructions.

Please see Addendum.

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.

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; E.O. 12333, as amended, United States Intelligence Activities; E.O. 12829, as amended, National Industrial Security Program; E.O. 10865, as amended, Safeguarding Classified Information Within Industry; E.O. 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13470, Further Amendments to Executive Order 12333; E.O. 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13526, Classified National Security Information; E.O. 13741, Amending Executive Order 13467, To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; E.O. 13764, Amending the Civil Service Rules; DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP); DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.Legal basis differs based on the mission purpose for which the data was collected. The originating information systems and/or governing SORNs and collections noted within the PIA maintain the legal bases/authorities. These authorities are provided through Privacy Act Statements at time of collection. As EDGC progresses, the number of inherited legal bases will expand.

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.

Please see Addendum.