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:

National Background Investigation Service (NBIS) Atlas Unclassified (Atlas-U)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

04/20/26

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
- ☒ 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 Defense Counterintelligence and Security Agency (DCSA) is responsible for the determination and continuous vetting of government and industry personnel in the areas of credentialing, suitability and national security. The 15 January 2021 memorandum from the Performance Accountability Council (PAC), "Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0", provides the milestones and implementation requirements to make Trusted Workforce (TW) 2.0 operational. Coordinated with Congress and the federal community, this memorandum levies three specific milestones relating to Personnel Vetting on DCSA encompasses Periodic Reinvestigation, Continuous Evaluation, and Continuous Vetting.

Atlas-U will be used by DCSA Personnel Vetting (PV) to perform low-side Expedited Screening (ES) workflows as well as the primary data source for low-to-high (and destination for high-to-low) connections with the higher classification NBIS ecosystem to meet TW 2.0 milestones. It shall provide the ability to ingest case management data; triage alerts; assign, manage, and execute case management workflows; retrieve and collocate data on cases to a single database; gather metrics; create reporting products for stakeholders; and archive, monitor and retrieve case 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)*

PII is collected for three primary reasons:
1) Identification: To establish who a person is, through a collection of certain identity attributes
2) Verification: To facilitate data sharing, personally identifiable information (specifically Social Security Number) is used to uniquely identify individuals to match their data with those of mission partners in order to create a comprehensive operational security view of the individual under investigation.
3) Mission Related Use: The PII is collected in support of Trusted Workforce (TW) and ES requirements, to determine if individuals pose a security risk. PII is collected in support of federal Background Investigations to determine the continued trustworthiness of individuals holding a security clearance. The primary mission uses (per the DoDI 1000.30) for which the collection of this PII falls is "Security Clearance Investigation or Verification" and "Law Enforcement, National Security, and Credentialing."

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.

The cleared individuals on whom the PII will be collected do not have the opportunity to object to Atlas-U's collection of PII, as they do not have access to the system. However, individuals give consent for PII to be collected when voluntarily submitting the SF85, SF85P, or SF86.

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.

Because the PII obtained by Atlas-U may be disclosed without the subject's consent as permitted by the Privacy Act [5 U.S.C. 552a(b)]; by routine uses (a list of which are published in the Federal Register for SORN DUSDI-02-DoD); and in accordance with memorandums of agreement with source agencies (such as with Executive Office of the President (EOP) Office of Administration (OA) as defined in the Sept 2020 MOA between EOP/OA and DCSA"); a subject may not have knowledge how their PII is being utilized, and as such, has no ability to consent to its usage.

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

This is not applicable, as individuals do not provide PII to Atlas-U directly. However, individuals are provided a Privacy Act Statement when voluntarily submitting the SF85, SF85P, or SF86.

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.	Personnel Vetting
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Military Services (Army, Navy, Air Force), Fourth Estate / Non-Service DoD under the DCSA purview, and Under Secretary of Defense for Intelligence.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Federal agencies/offices/establishments in the executive, legislative, or judicial branches of the Federal Government under the DCSA purview; Executive Office of the President (EOP) Office of Administration (OA).
☐ 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.	Enlighten, LLC and Personnel Vetting mission supporting DCSA contractors. The contract references DFARS 252.204-7012, and additional FAR Privacy Clauses being reviewed through contract verification/modification.
☐ 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

The following data sources will be used: SF85, SF85P, SF86, Defense Information System for Security (DISS), DNI Continuous Evaluation System (CES), DNI Scattered Castles (SC), Terrorist Identities Datamart Environment (TIDE), FBI Enterprise Vetting Center (EVC), DHS National Vetting Center (NVC), and Financial Crimes Enforcement Network (FinCEN). Data will also be received from the Executive Office of the President (EOP) Office of Administration (OA) as defined in the Sept 2020 MOA between EOP/OA and DCSA.

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)*

Atlas-U will connect to other NBIS systems: Data Management System (DMS), Defense Information System for Security (DISS), and the DCSA Enterprise Data Layer (EDL). Official forms collected will include SF85, SF85P, SF86, and Personnel Vetting Questionnaire (PVQ) data. The EOP/OA will also provide Subject PII and other relevant information to Atlas-U in a to be defined format agreed to in accordance with the Sept 2020 MOA between EOP/OA and DCSA.

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 DUSDI.02 DoD

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.

Note: Per the September 2020 MOA between EOP/OA and DCSA Section 5.1.1, the subset of records received from EOP/OA and temporarily stored within the system "are not DCSA records subject to the Federal Records Act but are subject to the Presidential Records Act, and are at all times relevant to this MOA under the exclusive legal custody and control of EOP/OA. As such, DCSA system of records notice DUSDI 02-DoD Personnel Vetting Records, 83 Fed. Reg. 52,420 (Oct. 17, 2018) does not apply to records produced or received by DCSA under this MOA."

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. DAA-0446-2019-0004 (BI and Internal Adjudications Record Schedule)

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

(3) Retention Instructions.

Decentralized copies shall be retained consistent with the guidance defined in applicable NARA General Records Schedules. Under NARA General Records 5.6, section 170, investigative reports and related documents furnished to an agency by the investigation service provider (ISP) should be destroyed in accordance with the ISP's instructions. DCSA instructs that decentralized records may be maintained only so long as the subject of the report remains of interest to the agency for the purposes defined in the DUSDI 02-DoD SORN (e.g. suitability, security, credentialing purposes). Upon separation or when the subject is no longer of interest to the agency, the agency must dispose of any/all background investigation records.

Information received from the EOP/OA are subject to the requirements specified in the Sept 2020 MOA between EOP/OA and DCSA, including but not limited to the following:
"5.1.2 EOP/OA is not subject to the Privacy Act, but is subject to the Presidential Records Act (PRA). Information received by the EOP/OA shall be considered a Presidential Record and maintained in accordance with the PRA."
"5.1.3 Transfer and Retention. In accordance with 36 CFR 1210, 1218(c), and 1270 et seq., the vetting and screening records shall be transferred to EOP/OA for the appropriate records retention in accordance with the PRA. Within 90 days of confirmed transfer to the EOP/OA, DCSA will dispose of the records and copies thereof."
"5.2.1 For individuals with dual affiliation, referenced in 4.1.6, DCSA will...transfer results to EOP, but will also retain the records pursuant to this MOA as required by applicable Federal laws, regulations, standards and applicable System of Records Notices, including Personnel Vetting Records System, DUSDI 02-DoD. The records retained by DCSA will remain the property of DCSA, and are subject to the provisions of the Freedom of Information Act, 5 U.S.C. section 552, as well as the Privacy Act of 1974, 5 U.S.C., section 552a.

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.

5 C.F.R. parts 2, 5, 731, 732, 736, and 1400 establish the requirements for agencies to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. Depending upon the purpose of

the particular background investigation, information collection is authorized under Executive Orders 9397, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12. DCSA is authorized by Executive Order (EO) 13764 and EO 13869 to provide background investigation services for the Federal Government, and has the capability to provide the requested services on a fee-for-service basis.

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.

DISS: 0705-0008 (expiration 11/30/2027)
PVQ: 3206-0279 (expiration 06/30/2028)
SF85: 3206-0261 (expiration 12/31/2027)
SF85P: 3206-0258 (expiration 04/30/2027)
SF86: 3206-0005 (expiration 11/30/2026)
NBIS: 0704-0622