

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:

FIELD WORK SYTEM (FWS)

2. DOD COMPONENT NAME:

Defense Counterintelligence and Security Agency

3. PIA APPROVAL DATE:

10/08/25

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 purpose of the Field Work System (FWS) is to provide special access for DCSA investigators, record checkers and support staff comprised of both federal employees and contractors located throughout the world, the ability to read, add, and update investigative data. FWS collects PII pertaining to individuals under investigation, including: first name, last name, address, phone number, aliases used, Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB), educational information, financial information, personal conduct, legal information, medical information, employment information, and other information requested and obtained in the background investigation process. In addition, FWS may contain information about individuals other than the subject of the background investigation, such as their spouse/cohabitant, close relatives, employers, doctors and other medical personnel, neighbors, and other individuals that the applicant identifies or who are identified by the investigator during the course of the investigation. FWS also may contains other historical information about the applicant that is obtained or developed in the course of investigation, which is information that is part of the subject's personal history.

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)

FWS supports the background investigation process by collecting, disseminating, and maintaining information about individuals under investigation, though it does not directly process Personally Identifiable Information (PII). It provides a centralized environment for investigators to access PII originating from the PIPS database and to gather additional or corrected PII directly from individuals when discrepancies are identified. Upon completion of a case, FWS facilitates the transfer of the entire case file, including all relevant PII, back to the PIPS database for continued use and analysis. FWS collects PII for identification and mission-related use for the personnel vetting process.

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 ability to object to the collection and use of their information directly in FWS. However, individuals who are the subject of an investigation are notified at the point of collection, at the beginning of an in person interview, and on various consent forms about why their information is being collected and the purposes for which it will be used.

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.

Individuals do not have the ability to consent to the collection and use of their information directly in FWS. However, individuals who are

the subject of an investigation are notified at the point of collection, at the beginning of an in person interview, and on various consent forms about why their information is being collected and the purposes for which it will be used.

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

Subjects do not have access to the FWS system. However, subjects and sources are provided a Privacy Act Statement when completing investigative forms and/or upon interview.

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 Personnel Vetting

☐ 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.)

Enlightened will ensure that all personnel comply in accordance with the Privacy Act of 1974, PII in 2 CFR Part 200.79, all applicable DCSA privacy policy guidance, related laws, regulations, policies, and requirements, Executive orders, Intelligence Community directives, and other applicable guidance to DoD Components conducting intelligence activities with respect to privacy and civil liberties matters (e.g., Executive Order 12333 and DoD Manual 5240.01).

Specify.

☐ 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

PIPS

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)

FWS collects PII only when discrepancies are identified or when PII is missing. The collection occurs during subject interviews, either by phone or in person. Once completed, the information is transferred to PIPS.

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 PERSONEL VETTING RECORDS SYS

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.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.

I. 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-0446-2019-0004-0002

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

(3) Retention Instructions.

PII is automatically deleted 30 days after the completion of the investigation. Users also have the capability to delete the PII within that 30-day period if it is no longer required.

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. 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.

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.

DoD Manual 8910.01 doesn't apply to pre-employment background investigations, as the data is collected from individuals as part of that process, not from the general public. If considered an internal collection, Volume 1 applies.