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:

OPM Personnel Investigations Processing System Imaging System (OPIS)

2. DOD COMPONENT NAME:

DoD Business Enterprise

3. PIA APPROVAL DATE:

03/08/22

Defense Counterintelligence and Security Agency (DCSA)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

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

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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 OPIS, the subject of this PIA, is to provide DCSA users with the ability to create, process, and produce standardized individual security investigation and background check products in a near-paperless work environment. The OPIS system allows DCSA personnel to electronically retrieve, modify, and store case documents that were previously only available on paper. The primary focus of OPIS is to provide imaging services in the form of paper to electronic document conversion, quality assurance, image storage and retrieval, and image release components.

There are multiple ways OPIS receives paper and electronic documents. The paper documents are scanned into OPIS, and electronic files are received from e-QIP, consumer reporting agencies, educational institutions, law enforcement agencies, and others and then ingested into OPIS. Once a case is closed, OPIS packages the appropriate documents for electronic delivery (eDelivery) to the sponsoring agency.

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)*

OPIS collects, uses, disseminates, and maintains images of the forms listed in Section 1.5 as well as other artifacts obtained from e-QIP, the requesting agency, DCSA Investigator or external sources in the background investigation process. These images contain PII about the subject of the investigation, including 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 on applicable forms and during the investigative process. In addition, in certain circumstances, the forms imaged contain the name, address, phone number, SSN, DOB, and POB for the individual's immediate family members, former spouses, and cohabitants, as well as information about others whom the individual identifies or who are identified by the investigator during the course of the investigation. OPIS also compiles and maintains a Distributed Investigative File (DIF), which is a compilation of releasable documents that are electronically transmitted to the customer agency.

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.

OPIS is a DCSA internal system not accessible by the public and/or individuals, therefore, notice is not given by the system itself. However, subjects of investigations are provided notice via Privacy Act statements at the original point of the information collection, and again at the beginning of an in-person interview.

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 are notified at the point of collection, at the beginning of an in person interview, and on various consent forms. They are informed that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of their background investigation. They do not have the ability, once they have agreed to the background investigation, to consent to some uses of their information and decline to consent to other uses. The exception to this is the SF86 Medical Release authorization, which is valid for 1 year from the date signed but can be revoked at any time by writing to DCSA, preventing further collection of medical information covered by that form.

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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

While individuals are not provided with notice specifically about OPIS, this risk is mitigated by the provision of Privacy Act Statements at various points of information collection. The Privacy Act Statement informs the individual on the uses of the information. While that statement does not explain the system specifically, it does provide information concerning how their information will be used. In addition, notification specifically about this system is provided through publication of this PIA.

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

[X] Within the DoD Component	Specify.	PIPS, NP2, NFW, eQIP
[X] Other DoD Components	Specify.	Once an investigation is closed, OPIS returns a specified set of images for eDelivery back to the sponsoring agency via secured connection. Appropriate MoUs and ISAs document each agency's responsibilities to protect the data in compliance with Federal Information Security Management Act (FISMA) 2014 guidelines. Roles and responsibilities regarding access to information are outlined in the MoUs and ISAs.
[X] Other Federal Agencies	Specify.	Once an investigation is closed, OPIS returns a specified set of images for eDelivery back to the sponsoring agency via secured connection. Appropriate MoUs and ISAs document each agency's responsibilities to protect the data in compliance with Federal Information Security Management Act (FISMA) 2014 guidelines. Roles and responsibilities regarding access to information are outlined in the MoUs and ISAs.
[ ] 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.	
[ ] 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

[X] 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)*

[ ] Face-to-Face Contact [ ] Paper

[ ] Fax [ ] Telephone Interview

[X] 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 DUSDI 02-DOD Personnel Vetting Recor

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. N1-478-08-002 and DAA-0446-2019-0004.

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

(3) Retention Instructions.

The records in OPIS are subject to the retention schedules referenced above. Depending on the type of information and the action taken on that information, various retention periods apply. Standard investigations
with no issues are retained for 16 years from the closing of the investigation; those with issues are retained for 25 years from the closing of the investigation. Files obtained from other agencies in the course of an investigation are retained consistent with the agreement between the agency and DCSA.

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.

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.

OPIS itself is not a public information collection; therefore it does not have an OMB Control Number. However, OPIS as a repository does contain images of several collections which do have OMB Control Numbers.
SF-85: Questionnaire for Non-Sensitive Positions 3206-0261 Expiration: 09/30/2021
SF-85P: Questionnaire for Public Trust Positions 3206-0258 Expiration: 12/31/2020
SF-85P-S: Supplemental Questionnaire for Selected Positions 3206-0258 Expiration: 12/31/2020
SF-86: Questionnaire for National Security Positions 3206-0005 Expiration: 02/28/2023