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:

DFAS Internal Review Case Management System

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

12/22/23

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
- [x] 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.)*

- [x] 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 DFAS Internal Review Case Management System (DIRCMS) is an investigations/law enforcement-specific case management system. DIRCMS will allow DFAS to achieve 100% compliance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards and to obtain parity with investigations counterparts. It will allow the DFAS Internal Review Criminal Investigation Branch (DICIB) to operate like peer agencies, track information, and gives the capability to retrieve that information on demand and upon request. The DICIB conducts investigations into criminal and administrative cases. Usage of the DIRCMS system focuses on information gathering to establish relevant facts to prove or disprove allegations of fraud and/or corruption.

The following PII elements are collected: biometrics, birth date, child information, citizenship, disability information, Department of Defense (DoD) ID number, driver's license, education information, emergency contact, employment information, financial information, gender/gender identification, home/cell phone, law enforcement information, legal status, mailing/home address, marital status, medical information, military records, mother's middle/maiden name, name(s), official duty address, official duty telephone, other ID number, passport information, personal e-mail address, photo, place of birth, position/title, Protected Health Information (PHI), race/ethnicity, rank/ grade, religious preference, records, security information, Social Security Number (SSN), work e-mail address, other financial information (assets, stocks, crypto-currency holdings, bankruptcy information, liens, etc.), protected health information (workers compensation information, health status, and payments for healthcare).

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)*

Verification, Identification, Data Matching, and Mission-Related Use.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

DIRCMS does not collect PII directly from the individual. PII maintained in the system is collected by other methods (other information systems, law enforcement databases, etc.), and is added to case files within the system by DFAS Internal Review Criminal Investigation Branch personnel.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

DIRCMS does not collect PII directly from the individual. PII maintained in the system is collected by other methods (other information

systems, law enforcement databases, etc.), and is added to case files within the system by DFAS Internal Review Criminal Investigation Branch personnel.

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

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.	All DoD OIG components that require access for mission requirements
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Military services, Investigative, and Auditing agencies throughout the DoD.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Law enforcement, Investigative, and Auditing agencies throughout the DoD.
☒ State and Local Agencies	Specify.	State and local agencies as needed for mission requirements
☐ 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

☒ Existing DoD Information Systems ☒ Commercial Systems

☒ Other Federal Information Systems

Law enforcement information: Ohio Law Enforcement Automated Data System (LEADS), Ohio Law Enforcement Gateway (OHLEG), and Enformion which provides data identity and investigation services.

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)*

During the course of an investigation, PII may be collected from many sources, both electronic and physical. This evidence may be in official forms/documents, financial statements, personal records, or other information deemed necessary to establish relevant facts to prove or disprove allegations of fraud and/or corruption.

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 TBD

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.

DFAS Privacy Office consulted DoD Privacy Office on 10/06/2023. DoD Privacy Office is in the process of coordinating with DoDIG to create a DoD-wide SORN to consolidate all administrative investigations that fall under the purview of the DoD.

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. DFAS 5015.2-M Volumes 1 and 2

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

(3) Retention Instructions.

SCHEDULE 7650 Rule 6, CASE MANAGEMENT LOG, Cut off at case closure. Destroy entries 15 years after cutoff but longer retention is authorized if required for business use.

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.

1) Public Law 95-452, as amended, Inspector General Act of 1978;
2) DoD Directive 5106.1, Inspector General of the Department of Defense; and
3) DoD Directive 5106.04, Combatant Command Inspectors General.

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.

This collection of information is exempt from an OMB collection number using exemption DoDM 8910.01, Volume 2, Enclosure 3, Item 8.a.(2).(b); which states: "During conduct of a civil action to which U.S. is a party, or during conduct of an administrative action, investigation, or audit involving government agency against specific individuals or entities".