

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:

Financial Accounting Management Information System (FAMIS) - Working Capital Fund (WCF)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

08/25/23

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.)

- | | |
|--|--|
| <input type="checkbox"/> From members of the general public | <input checked="" type="checkbox"/> From Federal employees |
| <input type="checkbox"/> from both members of the general public and Federal employees | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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 FAMIS-WCF is a turn-key Financial Management System Software (FMSS) solution. The solution is based on Oracle eBusiness Suite (EBS) R12.2.9 to support the following application family of products: General Ledger, Accounts Receivable, Accounts Payable, Federal Administration, Project Costing, Project Billing, Project Contracts, Purchasing, and Procurement. The system has implemented Oracle Identity and Access Management (IAM) to interface with EBS to provide Common Access Card (CAC) authentication to EBS. The PII being stored in FAMIS-WCF consists of Name(s), Social Security Numbers, Rank/Grade, Official Duty Telephone Phone, Financial Information, Work Email Address, Pay grade, Location code.

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)

FAMIS-WCF receives a data interface of travel obligation data multiple times per day from DTS. Data records are uniquely identified by truncated Social Security Number for the purpose of cost accounting, billing customers as required and recording financial transactions.

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 opportunity to object to the collection of their PII.

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 opportunity to consent to the specific uses of their PII.

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.)

- | | | |
|--|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory | <input type="checkbox"/> Not Applicable |
|--|--|---|

DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and claim for reimbursement.

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)

- | | |
|--|---------------|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. DISA |
| <input checked="" type="checkbox"/> Other DoD Components (i.e. Army, Navy, Air Force) | Specify. DFAS |
| <input type="checkbox"/> Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) | Specify. |
| <input type="checkbox"/> State and Local Agencies | Specify. |
| <input type="checkbox"/> 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. |
| <input type="checkbox"/> 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)

- | | |
|--|---|
| <input type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

FAMIS-WCF is not the authoritative source of PII. The systems collects and maintains time and attendance and travel obligation information via an interface file from DCPS and DTS where the initial collection and authorization of PII is performed.

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

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> In-Person Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> 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.

- Yes No

If "Yes," enter SORN System Identifier T7801

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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. GRS 1.1 #011
- (2) If pending, provide the date the SF-115 was submitted to NARA.
- (3) Retention Instructions.

Item 011: This system's outputs are accounting related transactions and reports. Disposition Instruction is temporary: Destroy when business

use ceases. Note: Other applicable guidance related to accounting files should be adhered to enable access by GAO, Office of the Inspector General, or other authority audit.

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.

The following authority allows Financial Accounting Management Information System (FAMIS) - WCF to collect the data: E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 12968, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; DoD Directive (DoDD) 5205.16, The DoD Insider Threat Program; DoD 5200.2-R, Department of Defense Personnel Security Program; DoDI 5200.02, DoD Personnel Security Program (PSP); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended. OMB Circular A-130 Circular establishes policy for the management of information resources, DoDI 8500.1, Cybersecurity, DoD 5200.1-R, Information Security Program, DoD 5200.08-R, Physical Security Program, DoD 5400.7-R, Department of Defense Freedom of Information Act Program, Public Law 100-235, Computer Security Act of 1987, (H.R. 145) January 8, 1988. GAO-09-232G Federal Information System Controls Audit Manual (FISCAM), GAO-08-81G, GAO-08-82G and GAO-07-313G Financial Audit Manual, Vol 1, 2 and 3 respectively.

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.

OMB CONTROL NUMBER: 0704-0577