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:

DISA FINANCIAL MANAGEMENT SYSTEM (DFMS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

02/12/24

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 production servers covered by this document are located at the DISA DECC Oklahoma City, Oklahoma. They support the following functionality provided by DFMS:
DISA Financial Management System
DISA Financial Dashboard
DISA Budgeting System
CFE Financial Statement Reporting

• The DISA Financial Management System (FMS) application is a custom-built web-based utilizing an ASP front-end and Oracle database for the backend. FMS supports the Planning, Programming, Budgeting and Execution System (PPBES) process for the Chief Financial Executive (CFE) division.

• The CFE Financial Dashboard (FDB) is a web-based portal based on the Commercial-off-the-Shelf (COTS) IBM Cognos Business Intelligence application. The Financial Dashboard provides a single point of access for Appropriated and DWCF financial data, standard operating procedures, policy documents, help documents, user guides, and useful links. The dashboard is maintained and administered by the CFE Financial Systems Division while the architecture is maintained by EIS.

• DISA Budgeting System (DBS) provides a effective document management for budget exhibits. The DFMS contains appropriated fund data used in the DoD Program Objective Memorandum (POM) and Budget Estimate Submission (BES)/President's Budget Performance Budgeting System (PBS) contains DISA Defense Working Capital Fund (DWCF) budget data used in the POM and BES, and feeds the DISA Financial Data Warehouse. For each budget phase within a budget cycle, the Comptroller's General Funds Division enters budgetary controls and Financial Managers enter supporting project-output funding.

The PII being stored in DFMS consists of Name(s) and Financial 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)*

User names are collected to identify owners of DFMS data.

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.

PII is required as part of the financial system and cannot be eliminated. The only PII that's stored in the FMS databases is the user's name, which is copied directly from their LDAP record.

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.

PII is required as part of the financial system and cannot be eliminated. The only PII that's stored in the FMS databases is the user's name, which is copied directly from their LDAP record.

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

A hard copy of the Privacy Act Statement describing the DISA practices regarding the use, maintenance, and collection of PII is provided to the individual submitting the complaint.

The Privacy Act of 1974 applies. The Contractor may be required to have access to highly sensitive and proprietary information for the performance of this Task Order. The Contractor shall not divulge any information about data processing activities or functions, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor shall observe and comply with the security provisions in effect at computer centers. Any required identification badges shall be worn and displayed at all times. A Department of Defense Contract Security Classification Specification, Form DD 254, must be completed. A DISA Non-Discloser Agreement (NDA) must be completed by each employee prior to commencement of work.

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.	DISA
☐ 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.)*	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

The existing LDAP user directory.

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)*

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 DoD-0015

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. 5.2, #020 Transitory and Intermediary Records

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

(3) Retention Instructions.

Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. DAA-GRS-2022-0009-0002

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.

The following authority allows DISA Financial Management System (FMS) application to collect the following data:
- MEMORANDUM FOR SERVICES DIRECTORATE: SUBJECT: (U) Interim Authorization to Operate (IATO) for DISA DFMS, eMASS System ID 11, DITPR ID 6010
- 10 U.S.C. Chapter 8: DoD Directive 5109; Defense Information Systems Agency (DISA)
- DoD Instruction (DoDI) 8510.01; SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

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: 0704-0415; Expiration Date: None