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 Management Information System

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

01/31/24

DHA J8, Business Integration

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 Financial Management Information System (FMIS) is an integrated resource execution system that enables the Military Health System (MHS) Resource Management users to rapidly compile operational data from disparate internal and external legacy financial, acquisition, logistics, personnel, and payroll data sources. This system also delivers consolidated information in standardized and user-defined reports to MHS Resource Managers and Resource Analysts via the FMIS web interface. FMIS allows the MHS to perform its mission of providing quality financial support for subordinate activities and headquarters which is critical to the overall mission of funds tracking.

The categories of individuals with PII/PHI in FMIS include: Military Personnel (Active Duty, Reserve, National Guard) for Army, Navy, Air Force; Federal Civilians (DoD, Army, Navy, Air Force, and Veterans Affairs); local nationals; federal contractors; volunteers. The types of Personally Identifiable Information (PII) collected are demographic and employment information.

FMIS is owned and operated by DHA J8, Business Integration.

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)*

The PII/PHI information is collected for identification purposes. Financial data is linked to the Electronic Data Interchange Personal Identifier (EDIPI) to track Individual workload and/or ensure individuals are properly aligned to facilitate organizational pay tracking.

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.

FMIS receives PII/PHI from system-to-system interface; therefore, the opportunity to object is only available at the source system.

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.

FMIS receives PII/PHI from system-to-system interface; therefore, the opportunity to object is only available at the source system.

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

Information maintained in the system of records is not collected directly from the individual.

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.	DHA Military Treatment Facilities
☐	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☒	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Department of Veterans Affairs
☐	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.	Contractor Name: Avosys Inc. and Idea Entity Inc. Performance Work Statement (PWS) Section 1.6.7.4: Privacy Act Compliance: The Contractor shall comply with FAR 52.224-1, Privacy Act notification, and FAR 52.2247-2 Privacy Act. Violation of the Privacy Act may involve the imposition of criminal penalties. Section 1.6.7.5: Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security: Per DoD 6025.18, the Contractor meets the definition of Business Associate and is required to comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the Contractor agrees to abide by applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and per DoD 6025.18 and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.
☐	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

Air Force Commanders Resource Integration System (CRIS); Air Force Defense Enterprise Accounting and Management System (DEAMS) Defense Civilian Pay System (DCPS); Defense Medical Human Resource System Internet (DMHRSi); General Fund Enterprise Business System (GFEBS); MHS Mart (M2); MHS Data Repository (MDR); MHS Information Platform (MIP).

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 0004

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. GRS 1.1, item 001 (DAA-GRS-2016-0013-0001)

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

(3) Retention Instructions.

FILE NUMBER: 206-13
DISPOSITION: Temporary. Cut off fiscally. Destroy 3 years after cutoff.

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.

Public Law 113–101, Digital Accountability and Transparency Act of 2006, as amended in 2014; Public Law 113–291, Federal Information Technology Acquisition Reform, 2015; 10 U.S.C. 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 10 USC 117, Readiness Reporting System; 10 USC 482, Readiness Reports; 31 USC 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 USC 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Directive 7730.65, Department of Defense Readiness Reporting System; DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense; DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense; and E.O. 9397, Numbering Systems for Federal Accounts Relating to Individual Persons, 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.

Information is not collected directly from individuals and is not considered public information collections per Encl 3, Para 8b(2).