

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:

Operational Data Store (ODS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

06/12/19

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
- 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
- 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.

To permit DFAS and Army financial managers the ability to retrieve, review and update financial payment information. Database records are also used for extraction or compilation of data and reports for budget execution status and statistical analyses for use internally or externally as required by DoD or other government agencies.

Personally Identifiable Information (PII) is collected from the following types of records: military pay, civilian pay, travel pay, vendor pay, Deployable Disbursing System (DDS), Automated Disbursing System (ADS), and System Authorization Access Request (SAAR) DD Form 2875 security clearance information.

The following types of PII information are contained in the ODS database: 1). Name. 2). Social Security Number. 3). Personal email address. 4). Mailing/Home Address. 5). Home/Cell phone. 6). Security Information. 7). Financial Information. 8). Employment Information. 9). Gender. 10). Marital Status. 11). Citizenship. 12). Place of Birth. 13). Race/Ethnicity. 14). Work E-mail Address. 15). Birth Date. 16). Position/Title. 17). Rank/Grade. 18) Child Information. 19) Official Duty Address. 20) Official Duty Telephone Phone.

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)

PII is collected in the System Authorization Access Request (SAAR)-web DD Form 2875 process for verification that the user is authorized access to the PII information contained in the ODS database.

The other PII, which is collected by existing DoD systems and interfaced to ODS, is collected to uniquely identify the individual in order to process payment transactions for the individual. The SSN PII information allows data matching to prevent duplicate payments to the individual. PII is collected to facilitate other systems ability to provide mandatory reports to the US Treasury.

The PII data intended use is to meet the DFAS fiduciary responsibilities related to payments and withholdings for individuals and corporate entities.

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.

With the exception of the ODS SAAR-web records list below, ODS does not collect PII directly from individuals but receives PII after it has been collected by another system such as Defense Joint Military Pay System – Active Component (DJMS-AC).

The SAAR-web Privacy Act Statement that is displayed to the user includes the following notification of their ability to object to collection: "Disclosure: Disclosure of this information was received from individuals voluntarily. However, their failure to provide the requested information may impede, delay or prevent further processing of payments by DFAS."

The ODS SAAR-web sub module collected SSN from individual system users during the period from the deployment of SAAR-web on July 27, 2008 through November 21, 2009. The SSN field is masked on those records. Also, SAAR-web contains PII which is the security clearance information.

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.

By signing the system access request form, the individuals consent to the routine and specific uses listed in the Privacy Act Statement on the 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.)

Privacy Act Statement Privacy Advisory Not Applicable

Authority: 5 U.S.C 301, Departmental Regulations, Department of Defense Financial Management Regulation (DoDFMR) 7000.14R, Vol 10; 31 U.S.C Sections 3512 and 3513; and E.O. 9397 (SSN) as amended.

Purpose of Use: Information collected in the SAAR DD Form 2875 is used for verification that the user is authorized to access the system. This access authorizes DFAS and Army financial managers the ability to retrieve, review and update financial payment information.

Database records are also used for extraction or compilation of data and reports for budget execution status and statistical analyses for use internally or externally as required by DoD or other government agencies.

Routine Uses: Those generally permitted under the 5 U.S.C 522 A(B) of the Privacy as required.

Disclosure: Disclosure of this information was received from individuals voluntarily. However, their failure to provide the requested information may impede, delay or prevent further processing of payments by DFAS.

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

Within the DoD Component

Specify. DFAS interface partners share data.

Other DoD Components

Specify. 1. US Army is the primary sharer of the PII data.
2. Defense Information System Agency (DISA) is provided PII data on: a). The DD Form 2875 for privileged users. b). On data files to Secure File Gateway (SFG) for file relays.
3. Other Defense Agencies: a) National Security Agency (NSA). b). Special Operations Command (SOCOM). c). Washington Headquarter Services (WHS), d). Department of Defense Education Activity (DODEA), e) Organization of the Joint Chiefs of Staff (OJCS). Defense Debt Management System (DDMS).

Other Federal Agencies

Specify. White House Management Office (WHMO)

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. No independent contractor access. Contractor access to ODS PII is only allowed to the extent it is authorized by the DoD component that sponsors the contractor.

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

Individuals do not provide SSN. But do provide other PII data on the SAAR-web, DD Form 2875, application. ODS interface partners provide PII data, including SSN, to ODS.

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 checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input checked="" type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

DD Form 2875 PII data is collected from ODS SAAR-web application customers when they request access to ODS. Other DD Form 2875s are completed outside of the SAAR-web application.

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

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.

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

(3) Retention Instructions.

Per NARA and DFAS 5015.2-M, Volume 2. Retention Instructions: Cutoff at the end of the fiscal year and destroy 10 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 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.

5 U.S.C. 301, Departmental Regulations, 31 U.S.C. 3512 and 3513, Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vols. 6A, 6B, and 10; E.O. 9397 Social Security Number (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.

Per DoD Manual 8910.01, V2, the system does not collect information directly from members of the public and therefore, there is no PRA requirement.