

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:

FM Workflow

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

12/03/20

Office of Financial Operations

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.

This system will enable the implementation of centralized records management across the AF Financial Service community. This system will also facilitate processing of financial transactions including Travel Pay (TDY); Retirement/Separation; Civilian Permanent Change of Station (CivPCS); Debts; and Disbursements.

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 information is collected to facilitate execution of electronic financial transactions. Information will be used to ensure military pay transactions occur. Administrative and mission use to effectively pay members with minimum delay.

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.

Yes however failure to furnish the requested information may result in total or partial denial of amount claim.

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.

Officers and employees of the agency which maintain the records have a need for the record in the performance of their duties IAW 5 U.S.C. 552a Section 3(b)(1).

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

Privacy Act statement is provided at point of collection. For example, the forms listed in section 2.j of this document.

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.

<input type="checkbox"/>	Other DoD Components	Specify.	<input type="text"/>
<input type="checkbox"/>	Other Federal Agencies	Specify.	<input type="text"/>
<input type="checkbox"/>	State and Local Agencies	Specify.	<input type="text"/>
<input checked="" 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.	Information Gateways, Inc and P3S Corp. Baseline IA controls implemented. Non disclosure statements in place for all contractors
<input type="checkbox"/>	Other (e.g., commercial providers, colleges).	Specify.	<input type="text"/>

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

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

eFinance Workspace and Financial Services Offices (FSOs).

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 type="checkbox"/>	Website/E-Form
<input type="checkbox"/>	Other (If Other, enter the information in the box below)		

DD 1351, DD 1351-2, DD 1351-2C, DD 1351-6, DD 2278, DD 1610, DD 1705, DD 2912, DD 1300, AF 899, AF 594, AF 220, SF 1199A, FMS 2231, W-4

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://dpcltd.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.

T 65 - 21 R 16.00-Travel Records (including Defense Travel System (DTS) and Reserved Travel System (RTS) Background Information); Destroy 10 years after period covered by account.
T-65 - 22 R 30.00: Collection and Disbursement
Destroy 1 year and 1 month after close of FY in which created, provided there are no outstanding discrepancies for which corrective action has been prescribed by HQ DFAS-DE.
T 65 - 30 R 01.00: Records Sent to HQ DFAS-DE; e.g., MPOs, Pay Adjustment Authorizations
Destroy after 6 months.

Note: Among the disposition cited in this field, the one with the longest retention time will be used on the systems records data. Since all records are tied to a travel voucher in FMWorkFlow the disposition would be 10 years. For example, collections and disbursements are not stand alone transactions they are linked to a travel claims.

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.

10 U.S. Code § 8022 – Financial Management; Department of Defense Directive 5118.05, Defense Finance and Accounting (DFAS); Air Force Policy Directive 65-1, Management of Financial Services, and E.O. 9397 (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.

Exempt from Paperwork reduction act OMB control number requirement. Does not collect from members of the public.

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|--|---|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Birth Date | <input checked="" type="checkbox"/> Child Information |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Gender Identification |
| <input checked="" type="checkbox"/> Home/Cell Phone | <input type="checkbox"/> Law Enforcement Information | <input checked="" type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input checked="" type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone Phone | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Records | <input type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input checked="" type="checkbox"/> Work E-mail Address | <input type="checkbox"/> If Other, enter the information in the box below | |

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

- Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

SSN Justification Memo submitted to DoD on 11/20/20.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

FMWF receives inbound transactions files from each Financial Services Office (FSO) to process and record entitlement payments and collections through RTS. The Unique Item Numbering requirements of these legacy systems are still dependent upon SSNs. Accordingly, FMWF is authorized to process unique SSN data based on DoDI 1000.30, enclosure 2, section 2.c(11). Legacy Systems Interface.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

FMWF has role-based system access to limit visibility of SSN data to individuals with duties and responsibilities associated to civilian and military pay analysts in the AF. Users with this information require an approved DD Form 2875 to control system access. The FMWF application is housed within the Network Control Center (NCC), 28 Communications Squadron (CS), Ellsworth AFB, SD.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
 If "No," explain.

- Yes No

Future mitigation will be based on requirements of travel and pay systems currently in use that require the provided PII. Until these systems reduce SSN usage, FMWF must provide as required.

b. What is the PII confidentiality impact level²? Low Moderate High

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.