



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Memorandum Fiscal Services (MFS)

Department of Navy - USMC - Marine Forces Reserve

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

MFS does not collect information on the public.

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

DFAS SORN T7207, General Accounting and Finance System - Defense Travel Records (GAFS-DTS) (March 25, 2014, 79 FR 16315) authorities:

5 U.S.C. 301, Departmental Regulations; DoD Directive 5118.5, Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vol. 4, Defense Finance and Accounting Service; 31 U.S.C. Sections 3512, Executive agency accounting and other financial management reports and plans and 3513, Financial reporting and accounting system; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose of MFS. The Memorandum Fiscal Services (MFS) is a web based financial integration system used for a variety of functional areas such as budgeting, fiscal reporting, accounting, transactional validation, and document processing. MFS receives daily financial data feeds from external systems and compiles this data with user-generated information to produce tailored management reports. In addition, MFS provides a streamlined platform for account and transaction validation where fund managers may use historical information for reconciling outstanding or abnormal accounting records. As part of the researching effort and one of the primary keys, Fund Managers use the truncated SSN as a unique identifier.

Description of PII. A truncated SSN for federal employees traveling on government-funds Orders is coupled with the traveler's name. MFS is not the collection point for the PII, the source systems are MCFIAS and MCORS.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Even a truncated SSN can pose a privacy risk if conjoined with other PII. If this PII is compromised, access to an individual's personal information (tax returns, medical, credit, etc.) could be made available for unauthorized use causing extreme hardship on the SSN owner.

The truncated SSN is not gathered/collected within MFS but is transferred via a Secured Gateway File (DISA Mechanicsburg, PA) connection from the source systems (MCFIAS and MCORS) to MFS. This constitutes a secure system-to-system data transfer.

MFS provides several layer for safeguarding PII. All users must access the system using a DoD-issued CAC authentication. Annual Privacy Act and Personally Identifiable Information (PII) training is required for all military, civilian, and contractor personnel to retain a valid CAC. Training is in compliance with DoD 5400.11-R "Department of Defense Privacy Program" 14 May 2007; OSD Memorandum "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)" 5 June 2009.

All reports extracted from MFS are labeled "For Official Use Only - FOUO".

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Fund Managers (FMs) responsible for the recording of valid transactions in the Marine Corps accounting system , SABRS, have a need to use the truncated SSN in the execution of their respective duties. The duties of the FM may include the reconciliation of outstanding transactions where the truncated SSN may become an important piece of the research criteria.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Contractor: H2 Performance Consulting Corporation. Contract Number: M67861-14-C-A002. Section H, IX. Release of Public Information. subparagraph d. Contractor personnel working at MARFORSPTFAC, New Orleans, LA may work with software and hardware capable of storing, processing, or transmitting Personally Identifiable Information (PII). Therefore, any of the contractors that are performing work on or in support of software and hardware capable of storing, processing, or transmitting PII are subject to the Privacy Act. The required FAR privacy clauses are in the contract and are also an integral part of the Statement of Work.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

PII is not collected in MFS as the source of origin. The Truncated SSNs for DoD personnel traveling on funded Orders are captured in two external systems: the Marine Corps Financial Integration Analysis (MCFIAS) and the Marine Corps Orders Resources System (MCORS). MFS receives the financial transactions (to include the truncated SSNs) via a system-to-system file transfer (Secure File Gateway) managed by DISA Mechanicsburg, PA. These two external systems would be the collection entry point where the individual would be offered the opportunity to object the collection of their PII.

j. 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 provide consent to use their PII in MFS. MFS is not the source of entry (collection) for the individual's PII (name & truncated SSN for travel records).

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|------------------------------------------------|-------------------------------------------|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

PII is not collected within MFS. It is transferred to MFS as part of a system-to-system daily data transfer. MFS receives truncated SSNs from MCFIAS and MCORS.

NOTE:

Sections 1 and 2 above are 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 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.