



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Fund Administration and Standardized Document Automation (FASTDATA)

Department of the Navy - DON/AA

### 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**

**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.

FASTDATA Web implemented the OPM requirements for the SF182 training document. Defense Finance and Accounting Service requires a SSN for EFT payments on SF1164 vouchers.

SF182: 5 U.S.C. § 4115, a provision of The Government Employees Training Act. PL 93-579, Section 7 (b); and E.O. 9397 (SSN), as amended.

SF1164: 5 U.S.C. Chapter 57 Federal Travel Regulations (FPMR 101-7); E.O. 11609; E.O. 11012; 26 U.S.C. 6011(b) and 6109; 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.

FASTDATA provides the SF182 document number and proper line of accounting for obligating funds and billing for training of DoD employees. Trainee SSN, DOB, Home Address and Phone are optional information in Section A of the form. When entered, the data is encrypted and, by default, the application will display only the last four digits when printing. The comptroller user has the option of displaying the SSN if needed when printing. Comptroller personnel provide enough information to satisfy local human resources requirements to support the individuals training plan and training completion status. The comptroller user has the same option for the SF1164 voucher. Defense Finance and Accounting Service has indicated the need for the SSN to set up EFT payments for the individual. In many cases, the individual creates the SF182 or SF1164 outside of FASTDATA and sends to the comptroller. FASTDATA provides the ability to record these as memo documents without capturing the PII information. FASTDATA does not use PII information to retrieve data. Key elements are financial to include the document number as primary.

When using FASTDATA to create the documents, you can potentially collected Name, SSN, truncated SSN, mailing/home address, birth date, home phone number, disability information, office email, office mailing address, office telephone number, position, title, payment and expenditure information, course training information. (See Section 3a).

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

The data in FASTDATA is not transmitted to any other system. Privacy Act fields are encrypted as required for data at rest. By default the SSN is truncated, when printed on the SF182 or SF1164, unless option to print full SSN is selected. Printed SF182s are sent to the Command human resources offices by the digitally signed emails (not part of the application functionality), hardcopy, or fax. SF1164s are sent to DFAS by fax, as they will not accept them by any other method.

Commands mitigate use of PII with Command credit card rather than individual credit cards for charges to cover various training or conference scenarios. Documents created outside of FASTDATA are handled by physical controls.

The following elements can potentially be collected: Name, SSN, truncated SSN, mailing/home address, birth date, home phone number, disability information, office email, office mailing address, office telephone number, position, title, payment and expenditure information, course training information.(See Section 3a).

**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.

**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.

**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.

Person provides the information to comptroller personnel to initially create the SF182 for securing the class or to get reimbursed through the SF1164.  
The employee can object and the command will eliminate the truncated SSN. Employee uses document to get credit for their training with Human Resources. SF1164s created when the individual insists on using the local claim vice using Command credit cards for items require reimbursement and direct deposit by DFAS. DFAS will not produce checks for reimbursement and require SSN for the direct deposit.  
Failure to provide the required information may delay or prevent credit and/or reimbursement.

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

**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 understand the use and requirements to secure training classes for career development or to get reimbursed. Once the information is collected these forms are used for those purposes only.

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

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

Describe each applicable format.

A Privacy Act Statement is part of the SF182 and SF1164

**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.**