



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Standard Accounting and reporting Systems (STARS)

Defense Finance and Accounting Service (DFAS)

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.

5 United States Code (U.S.C.) 301, Departmental Regulations; Department of Defense Financial Management Regulation (DoD FMR) 7000.14-R, Vol. 5; 31 U.S.C. Sections 3511, Prescribing accounting requirements and developing accounting systems; Section 3512, Executive agency accounting and other financial management reports and plans; 31 U.S.C. 3513, Finance Reporting and Accounting System; and Executive Order (E.O.) 9397 relating to federal agency use of social security numbers (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.

The Standard Accounting and Reporting System (STARS) is a general fund accounting, reporting and entitlement system. Navy Users record and account for Navy, Marine Corps, Air Force and Defense Agencies funds appropriated by Congress. The receipt and use of these funds are recorded from allocation to disbursement through structured successive steps. STARS currently supports many individual appropriations. STARS accounts for Navy - Departmental, Navy - Field, Marine Corps - Departmental, and Defense Agencies Field.

STARS consists of two sub-systems:

1. Field Level (STARS FL) - Navy Field Level Accounts Receivable and Accounts Maintenance
2. Headquarters (STARS HQ) - Navy Major Command (MAJCOM) Accounts Receivable and Accounts Maintenance

STARS FL and STARS HQ contains names, addresses, social security numbers (SSNs), truncated SSNs, and credit card data. The information is received by the STARS systems through secure file transfers from other DFAS accounting and pay entitlement systems. This information is maintained within the STARS system and cannot be retrieved using a personal identifier.

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

The result of mishandling personal data may lead to lost, stolen or compromised personally identifiable information (PII) which could be harmful to the individual in many ways (e.g., identify theft, damage to the individual's reputation and /or financial hardship). Such incidents could cast Defense Finance and Accounting Service (DFAS) in an unfavorable light to the public. Hence, access is limited to persons authorized to service or to use the system in performance of their official duties (requires screening and approval for need to know). DFAS adheres to physical protections of PII as described in accordance with DFAS5200.1-R. DFAS8400.1-R prescribes protection requirements for sensitive data, to include PII, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS8500.1

STARS data is exempt from mandatory release to the public under the Freedom of Information Act (FOIA). Protective measures are in place to separately safeguard PII data with access restricted on a "need to know" basis. Screens and reports that contain PII data have the following marking: THIS REPORT CONTAINS 'FOR OFFICIAL USE ONLY' (FOUO) INFORMATION. THIS REPORT MAY CONTAIN SENSITIVE INFORMATION COVERED BY THE PRIVACY ACT OF 1974. Defense Information Systems Agency (DISA) provides Secure File Gateway (SFG) relay to ensure adequate protection of data during system to system transfer processing. Protective measures are in place to separately safeguard PII data with access restricted on a "need to know" basis. Standard features of the SFG include certified in-flight and at-rest encryption, and enables public key enabled (PKE)/public key infrastructure (PKI) enforcement between each enclave. Furthermore no PII records in DFAS are processed or stored on mobile computing devices or removable electronic media.

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.

Information will be shared with the Department of the Navy. Information may be shared with law enforcement for investigative purposes.

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.

The STARS feeder system Defense Civilian Payroll System (DCPS) procedures provide individuals with the opportunity to object to the collection of the information. When personal information is collected for DCPS, either by hard copy or web-based applications, the individuals are provided a Privacy Act Statement that informs them that providing the information is strictly voluntary.

(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.

Information is stored in the STARS system; no retrieval. The information is collected in STARS FL and STARS HQ solely to record obligations for labor costs. This information is maintained within the STARS system and cannot be retrieved using a personal identifier.

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

- Privacy Act Statement** **Privacy Advisory**
 Other **None**

Describe each applicable format.

Defense Civilian Payroll System (DCPS) feeder system for STARS collects the personal information covered by the Privacy Act. When personal information is collected for use in DCPS, a Privacy Act Statement or Privacy Advisory is provided either on the form used to collect the data or on the web-based application used to collect the information.

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.