



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Facilities Information System 2.0 (FIS)

Department of the Navy - NAVFAC

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.

SORN T7335 authorities:

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. Chapter 53, 55, and 81; and E.O. 9397 (SSN).

SORN T7335D authorities:

5 U.S.C. 301, Departmental Regulations; DoD Directive 5118.05, Defense Finance and Accounting Service; DoDD 7000.14-R, Department of Defense Financial Management Regulation (DoDFMR), Vol. 4, Accounting Policies; 31 U.S.C. Sections 3512, Executive agency accounting and other financial management reports and plans; 31 U.S.C. 3513, Financial reporting and accounting system; and E.O. 9397(SSN), as amended.

Other authorities:

10 U.S.C. Chapter 5013, Secretary of the Navy
DoD Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 4 and Vol. 8

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 NAVFAC Facilities Information System (FIS) provides a single system for management of core financial and facilities information in support of General Fund mission execution. FIS interfaces with our accounting, real property, contract management, acquisition, and other systems to insure timely and accurate execution of worldwide NAVFAC mission objectives. Managing indirect costs such as Labor, Travel, Printing, and Training costs are included in the management of overall financial information. A portion of the financial data collected in FIS is Civilian and Foreign National Labor Costs by employee. The name and social security number (SSN) of these employees are carried for verification, correction, and adjustment purposes along with financial and employment information.

Personal information collected: Name, SSN, Financial information, Employment information.

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

The risk associated with the collection of the employee and SSN data is the possibility of inadvertent release of that data. To safeguard privacy, all access to FIS is secured by CAC and User-ID/Password methods approved by NAVNETWARCOM. Access to data by any authorized FIS user is limited to those with a need-to-know and secured by system 'Role Codes' that are administered by FIS System Administrators. Actual PII data in the FIS database is encrypted using a 128-bit encryption scheme to avoid ad-hoc querying of the data.

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.

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

Personal information is not collected from the individual.

All individuals with PII data managed in FIS are NAVFAC employees paid through Defense Civilian Payroll System (DCPS) and their Labor distribution is through FIS. There is no process for consent or objection.

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.

All individuals with PII data managed in FIS are NAVFAC employees paid through Defense Civilian Payroll System (DCPS) and their Labor distribution is through FIS. There is no process for consent or objection.

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.

Name, SSN and financial information within the Labor detail records are received from the Defense Civilian Payroll System (DCPS).

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.