



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

IEFACMAN GATEWAY AND REPORTING APPLICATION  
(IEFACMAN GATEWAY)

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 authorities:

SORN NM05000-2:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).

SORN N05230-1:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; CNICINST 5230.1, Total Workforce Management Services; OPNAVINST 3440.17, Navy Installation Emergency Management Program and E.O. 9397 (SSN), as amended.

SORN DPR 34 DoD:

5 U.S.C. 301, Department Regulations; 5 U.S.C. Chapter 11, Office of Personnel Management; 5 U.S.C. Chapter 13, Special Authority; 5 U.S.C. Chapter 29, Commissions, Oaths, Records, and Reports; 5 U.S.C. Chapter 31, Authority for Employment; 5 U.S.C. Chapter 33, Examination, Selection, and Placement; 5 U.S.C. Chapter 41, Training; 5 U.S.C. Chapter 43, Performance Appraisal; 5 U.S.C. Chapter 51, Classification; 5 U.S.C. Chapter 53, Pay Rates and Systems; 5 U.S.C. Chapter 55, Pay Administration; 5

U.S.C. Chapter 61, Hours of Work; 5 U.S.C. Chapter 63, Leave; 5 U.S.C. Chapter 72, Antidiscrimination; Right to Petition Congress; 5 U.S.C. Chapter 75, Adverse Actions; 5 U.S.C. Chapter 83, Retirement; 5 U.S.C. Chapter 99, Department of Defense National Security Personnel System; 5 U.S.C. 7201, Antidiscrimination Policy; minority recruitment program; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E. O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; 29 CFR part 1614.601, EEO Group Statistics; and E. O. 9397 (SSN), as amended.

SORN NM07421-1:

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).  
Statue Authority to collect Information.

**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 purpose of the ieFACMAN system is to facilitate management of mission related projects and contracts of the Naval Facilities Engineering Command. ieFACMAN is an enterprise system with business and support centric modules, including eProjects, eContracts, an integrated data store (iDS), eClient, and Total Force. The Total Force module is used for administrative purposes including the assignment of activity personnel (civilian, military, and contractor) to projects and contracting teams and computation of associated salary expenses. It goes further and assists activity management in the areas of readiness planning, workforce development, and disaster preparedness by storing employee specific data, including some PII data. The data contained in the system is typically aggregated and used for the preparation of such things as: telephone directories and emergency contact lists; Intelligent Workbook (IW) out-year planning reports; demographic data for assessing the age, diversity, disability accommodation needs, education levels, professional certifications, and skills level of our workforce; and damage assessment and response teams emergency recall lists. All reports and lists are labeled For Official Use Only (FOUO) and have access restrictions based on supervisory chains or an official need to know.

Personal information collected: Name, other names used, SSN, citizenship, gender, race/ethnicity, birth date, personal cell phone number, home telephone number, personal email address, mailing/home address, security clearance, spouse information, child information, financial information, disability information, employment information, military records information, emergency contact information, education information, and professional certificates.

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

There are numerous Security Controls in place restricting use to those users with an official need to know. Multiple forms of authentication are required to access the application data. All reports and lists are labeled For Official Use Only (FOUO) and also have access restrictions based on supervisory chains and an official need to know.

**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. NAVFAC Associates with need-to-know - Supervisory Chains, Business Line Leaders, and Community Managers

**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. VSolvit LLC. Safeguards for shared data are covered in Non-Disclosure Forms and SAAR-n forms. The Privacy Act FAR Clause is included in the Enterprise Business Support (EBS) contract. The Privacy FAR Clause will be added next time the contract is revised.

**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.

For PII data that is provided by the employee, the system is blank unless the employee chooses to enter the data or provides it to the system administrator for entry. PII data elements obtained via a TWMS interface were provided by the employee to OPM under their Declaration for Federal Employment in which they were advised of the likelihood of further disclosure in systems managing General Personnel Records.

(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.

Tacit consent evolves from the signing of the Declaration for Federal Employment form. PII data is provided to management in aggregate report formats for the purpose of accomplishing specific mission related taskings and are labeled FOUO.

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

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

Describe each applicable format.

Privacy Act Statement from Application Banner and Privacy Advisory from the Login Screen.

**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.**