



PRIVACY IMPACT ASSESSMENT (PIA)

For the

iNAVY (Navy Enterprise Intranet)
Department of the Navy - NAVSEA

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:

5 U.S.C. 301, Departmental Regulation
DoD Directive 5105.19, Defense Information Systems Agency (DISA)

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 this data system is to provide collaboration options for Navy Commands. Data falls into two categories, Unstructured and Structured. Unstructured - The collaboration data system allows for the storage of electronic files. These files may contain any nature of PII and are subject to appropriate privacy data handling requirements. Structured - Data collected at the gateway level is provided to support SharePoint Account self-enrollment and provisioning. Microsoft Forefront Identity Manager (FIM) is a state-based identity management software product, designed to manage users' digital identities, credentials and groupings throughout the lifecycle of their membership of an enterprise computer system. FIM integrates with Active Directory and Exchange Server to provide identity synchronization, certificate management, user password resets and user provisioning from a single interface. In the iNAVY implementation, FIM leverages information on the Common Access Card (CAC) and information stored in the (NAVY) Active Directory to allow user self-enrollment resulting in creation of an iNAVY (SharePoint) account. After the user submits the information, the request is routed to an authorized approver to validate prior to the account being generated. This data is being provided via a Identity Synchronization Service (IdSS) Machine Interface (IdMI). Multiple data elements of personnel information may be populated in each contact record.

Personal information collected and validated from individual CAC which includes: Structured: Name, office e-mail, Electronic Data Interchange Person Identifier (EDIPI), User Principal Name (UPN), Organization, Country, Certificate Issuer and Signature issuer, Unique Identification Code (UIC), and Business Telephone. Note: the site may contain other unstructured personal information posted by users.

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

Unstructured - Data files stored on the collaboration system by Tenant users are limited by logical controls a to data types and storage methodologies and this is enforced by continuous monitoring of content stores. Tenant users are prohibited from utilizing the platform for collection of PII. Structured - Account data is limited to identity information related to the individual's office persona(s) and environment. No other data of a personal nature is included. The data will not be copied or maintained in other systems for other purposes, such as for local physical access authorization systems, or for attribute-based access control (ABAC) systems. Data access will be restricted to authorized and authenticated system administrators and other implementation and maintenance personnel. All access by these personnel will be logged and periodically audited. Users of this data will be CAC authenticated and restricted to viewing only the appropriate data (such as user contact information in the address list).

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.

Data is collected by the Defense Enrollment Eligibility Reporting System (DEERS) system as part of standard personnel processing procedures at the time of receiving a Common Access Card (CAC).

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.

Data is collected by the Defense Enrollment Eligibility Reporting System (DEERS) system as part of standard personnel processing procedures at the time of receiving a Common Access Card (CAC).

Information is not collected directly from the individual.

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.

Pop-up Banner ----- Department of Defense: Terms of use.

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.