



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Secretariat Automated Resource Management Information System (SARMIS)

NAVY DON/AA OIT

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

10 U.S.C. 5013 - DoN Internal administrative requirements.

10 U.S.C. 5014 - Office of the Secretary of the Navy.

10 U.S.C. 5025 - Financial Management.

DoD 7000.14-R - DoD Financial Management Regulations (FMR) establishes requirements for administrative control of appropriations (of which payroll is a subset).

NAVSO P-1000 DoN Financial Management Policy Manual (FMPM) establishes DON/AA as Echelon 2 Major Financial Command.

SECNAVINST 5430.7Q - Assignment of responsibilities and authorities in the Office of the Secretary of the Navy. (Cancels 5430.7P)

SECNAV Memo 15JUN2010 - Establishment of the Department of the Navy Assistant for Administration (DON/AA).

SECNAVINST 7000.27A - Mandates, under 31 USC 1341 or 31 USC 1517, a qualified comptroller to report directly to the head of an activity. Additionally, designates overall responsibility to Comptroller for all matters related to financial management, including maintaining appropriate internal controls established for Financial Management within the organization.

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.

This is a Financial Management System that is critical to the Comptroller's ability to execute statutory, OSD, DON and agency mandated financial management duties during the Planning, Programming, Budgeting and Execution of resources. The resources managed include civilian personnel, military manpower and financial data. The management responsibilities include submission of requirements to higher authority, and allocation of resources to activities within the organization. Personal information-- individual's full name, SSN, gender, civilian pay and leave records-- is included in data from other systems in order to capture accurate accounting and recording of pay to civilian employees, to track organizational structures, and to reconcile civilian payroll charges back to budgeted cost centers for financial analysis.

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

The principle of least privilege is employed tightly throughout the system with multiple layers of access control. Users are required to acknowledge and sign a System Authorization Access Request form (DD FORM 2875) and SARMIS Account Request Form, which include a Privacy Act Statements and non-disclosure of information agreement. Access control measures include: storage in an office building protected by guards; storage in an office space protected by a digital cipher lock and blast-proof door; controlled screening; ID badges; and CCTV. Database access control measures include: use of visitor escorts; electronic access controls, such as CAC enabled computers and passwords; access to records limited to screened individuals cleared on a need-to-know basis in the performance of their duties; passwords to access system data; and periodic sweeps to delete inactive accounts. Additionally, although SSNs are in the database because they are required for data matching to track payroll charges back to budgeted cost centers for financial analysis, SSNs are not available from the application. The information is retained for 5 years in a secure location. At the end of the 5 year term, the information is destroyed.

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.

all federal PIA requirements.

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.

The system does not collect any data directly from the individual. Payroll data is received from the Navy Payroll system. The collection of SSN and payroll data is required for Navy payroll processing and analysis.

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 in the SARMIS system is pulled from other systems, not directly from individuals.

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

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

Describe each applicable format.

PII is not collected directly from the individual for this application. When an individual is employed by the Navy, the forms they complete when supplying their PII data contain a Privacy Act Statement.

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.