



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Warehouse Analytical Reporting System (WARS)
--

Department of the Navy - NAVAIR

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:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
E.O. 9397 (SSN), as amended
5 U.S.C. Chapter 11
Office of Personnel Management:
13, Special Authority
29, Commissions, Oaths and Records
31, Authority for Employment
33, Examination Selection, and Placement
41, Training
43, Performance Appraisal
51, Classification
53, Pay Rates and Systems
55, Pay Administration
61, Hours of Work
63, Leave
72, Antidiscrimination, Right to Petition Congress
75, Adverse Actions

83, Retirement
99 Department of Defense National Security Personnel System
SECNAV Instruction 12250.6, Civilian Human Resources Management in the Department of the Navy
The National Defense Authorization Act (NDAA) 2010 (H.R. 2647, Pub. L. 111-84, 123 Stat. 2190.)
Title 5, U. S. Code Sections 1104, 3321, 4305, and 5405
Executive Order 12107

Other authorities:

5 U.S.C. Section 301 - Government Organization and Employees Departmental regulations
5 U.S.C. 7201 - Government Organization and Employees, Antidiscrimination policy
10 U.S.C. 136 - Armed Forces, Under Secretary of Defense for Personnel and Readiness
Executive Order 9397 - Numbering System for Federal Accounts Relating to Individual Persons
Executive Order 9830 - Amending the Civil Service Rules and Providing for Federal Personnel Administration
29 CFR 1614.601 - EEO Group Statistics
EEOC Management Directive 714 - Instructions for the Development and Submission of Federal Affirmative Employment Multi-Year Program Plans, Annual Accomplishment Reports, and Annual Plan Updates.

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.

WARS provides NAVAIR with a source for historical data to do analytical processing and reporting. This system provides restructuring, integration, and capturing of summary level management information from a multitude of diverse transactional systems across functional business areas (i.e. planning, financial, personnel, acquisition). This data repository allows managers to obtain such data to develop corporate decisions and strategy based on the current environment, as well as, historical trends. WARS allows the organization to exploit information already captured in transactional systems and use the data for forecasting, trend analysis, and analytical processing. WARS is currently in a maintenance life cycle phase.

Data is obtained from official source systems including Navy ERP and the Defense Civilian Personnel Data System (DCPDS).

WARS performs a one-time collection of personal information via an individual's digital signature during the account creation process. This information includes name and DoD ID number and is used to provide certificate-based authentication in the system. WARS does not collect any other personal information directly from an individual.

Personal information collected includes: Name and other names used, SSN (full and truncated), DoD ID number, citizenship, gender, race/ethnicity, birth date, place of birth, mailing/home address, security clearance, financial information, disability information, employment information, education information, personnel actions, labor costing amount, awards, travel, and position information.

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

The perceived threats of the data stored and used are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.). All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that WARS, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place. Since WARS operates on the NMCI Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset. All systems are vulnerable to "insider threats". WARS managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should

have access to WARS. These individuals have gone through extensive training, extensive background and employment investigations.

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.

Naval Air Systems Command (NAVAIR), NAVAIR Total Force Office, NAVAIR Legal Office, Naval Sea Systems Command (NAVSEA), Naval Supply Systems Command (NAVSUP), Space and Naval Warfare Systems Command (SPAWAR), SYSCOM Competency Management, SYSCOM Comptroller and Business Financial Managers, SYSCOM Program Management, Strategic Systems Programs (SSP), Office of Naval Research (ONR), DON Human Resource departments and administrators, STRL Program Office, and Commander Naval Installations Command.

Other DoD Components.

Specify.

DoD Human Resource Organizations

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.

WARS collects personal information via individuals digital signature, which includes name and DoD ID number, in order to utilize this information to provide certificate-based authentication in the system. WARS does not collect any other personal information directly from individuals.

Individuals can object to the collection of PII by denying to submit digitally signed e-mail. If individual denies collection of PII, access to the WARS system is denied.

(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.

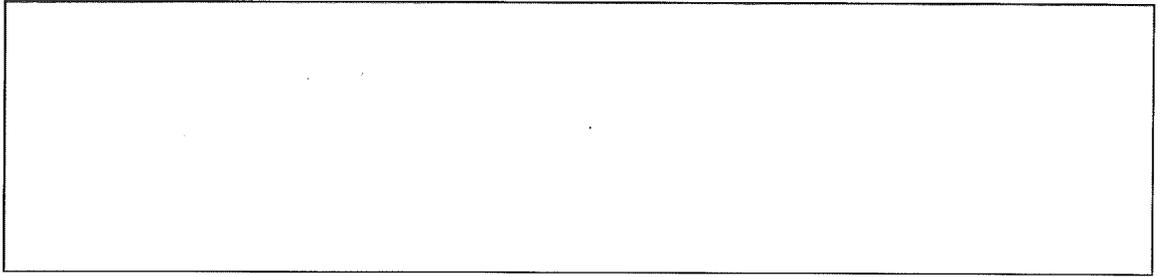
Consent is obtained at the official source systems. Individuals consent to uses of their PII data when data is collected for the official source system and by submitting a digitally signed e-mail during account request process.

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.

Data in WARS is obtained from official source systems and by individuals submitting a digitally signed e-mail.



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.