



PRIVACY IMPACT ASSESSMENT (PIA)

For the

NAVAIR Depot Maintenance System (NDMS)
--

Naval Air Systems Command (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.

5 U.S.C 301, Departmental Regulations; 5 U.S.C Chapter 53, 55, and 81
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).

DoD Financial Management Regulation (DoDFMR) 7000.14-R; Volume 4: Accounting Policy and Procedures; Volume 8: Civilian Pay Policy and Procedures; Volume 11B: Reimbursable Operations, Policy and Procedures - Working Capital Funds

Defense Finance Accounting Service (DFAS); Defense Industrial Financial Management System (DIFMS) Privacy Impact Assessment; Dated: February, 2009 -- Identifies NAVAIR Depot Maintenance System (NDMS) Time and Attendance (TAA) as an authorized financial feeder system.

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 NAVAIR Depot Maintenance System (NDMS) is a system of systems. One subsystem of NDMS is Time And Attendance (TAA), which is a Defense Industrial Financial Management System (DIFMS) financial feeder system. NDMS and TAA are referred to in the DIFMS PIA. the NDMS TAA subsystem maintains time and attendance data and labor distribution data as listed in Section 3a(1). TAA information sent to DIFMS is used by the Defense Finance and Accounting Service (DFAS) as payroll data.

The following PII data is collected:

Name; SSN; Other ID Number (i.e. Payroll Number) ; Mailing/Home Address; Security Clearance; Financial Information; Employment Information; and Other: (Leave Accrual, Series, Grade, Work Location, Job Order Number, Task Order Number, Occupational Series, Pay Period Identification, Time Card Certification, Special Pay Categories, and Work Schedule)

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

The NDMS TAA subsystem receives PII data entry and uses this PII for recording work accomplished by civilian, military, and contractor employees. In addition, NDMS TAA feeds DIFMS the specific information necessary to perform accurate payroll processing for an activities civilian employees.

In order to safeguard privacy PII information, entry and viewing is exclusively limited to the NDMS TAA Employee Master Record screen, which is controlled by a NDMS TAA privileged account access. This privileged account is only provided to personnel with a 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.

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.

Employees must read and sign a Privacy Act Statement as part of the new hire checklist. They can object at this point to providing the PII requested, but if they do not provide the PII they cannot be paid.

(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.

Employees must read and sign a Privacy Act Statement. At the time they have the ability to designate which data they do or don't want released. Should an individual refuse to disclose privacy data, that person cannot be paid.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

[Empty rectangular box]

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.

The PIA document is an HRSCE 5211/1 (new 1/99) form titled "DISCLOSURE OF YOUR SSN UNDER PUBLIC LAW 93-579 Section (b)". This form is presented as a paper document that must be signed by the individual being asked to provide PII data.

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.