



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Comptroller Document Management System (CDMS)
---

Department of the Navy - NAVAIR - Naval Air Warfare Center Aircraft Division
--

### **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. 5701-5757, Travel, Transportation, and Subsistence  
10 U.S.C. 135, Under Secretary of Defense (Comptroller)  
10 U.S.C. 136, Under Secretary of Defense (Personnel and Readiness)  
DoD Directive 5100.87, Department of Defense Human Resources Activity  
10 U.S.C. 5013, Secretary of the Navy  
10 U.S.C. 5041, Headquarters, Marine Corps  
DoD Financial Management Regulation 7000.14-R, Vol. 9, Travel Policies and Procedures  
DoD Directive 4500.09E, Transportation and Traffic Management  
DoD 4500.9-R, Defense Transportation Regulation, Parts I-V; 41 C.F.R. 300-304, Federal Travel Regulation  
Joint Federal Travel Regulation (Vol. 1) (Uniformed Service Members)  
Joint Travel Regulation (Vol. 2) (DoD Civilian Personnel)  
E.O. 9397 (SSN), as amended

**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.

Archive and retrieve personnel records, travel orders, and information concerning government-issued credit cards used for travel expenses. Personal info in databases includes Name and SSN (in most cases last 4 digits).

In the document images archived in the system, however, information includes:

Name, SSN, and in some cases Work Phone, home phone, home address, and email address.

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

Risk is exposure of Name, SSN, and in some cases Work Phone, home phone, home address, and email address.

Risk is minimal, because:

Data is stored on NMCI servers, secured by CAC authentication, with physical security enforced by NAVAIR IT/IM at building 1490. The CDMS System is only available to authorized users who have been approved by the data owners at NAWCAD Comptroller; permissions are restricted to a small subset of CDMS users based on need to know, again approved by the data owners, enforced by CAC authentication and NMCI Active Directory permissions. There is NO access to CDMS outside of NMCI.

**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. PII only accessible to employees and contractor support of NAWCAD and NAWCWD Comptroller.

**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. Booz Allen Hamilton, Inc - All support employees sign a Non-Disclosure Agreement and will attend PII training annually.

**Other** (e.g., commercial providers, colleges).

Specify.



**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.

PII is not collected directly from the individual.

**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.**