



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Employee Central Training Management System (EC/TMS)
--

Department of the Navy - NAVAIR - FRC Southeast, Jacksonville, FL

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 New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

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 function, composition
OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS)
Catalog of Navy Training Courses and Student Reporting Requirements
MCO 1580.7D Schools Inter-service Training
E.O. 9397 (SSN), as amended

Other authorities:

FRCSEINST 3500.2, TRAINING AND EMPLOYEE DEVELOPMENT

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 program maintains a current personnel listing and tracks and maintains training records for all personnel in order to report required training.

Personal information collected includes: Name, SSN, Payroll ID#, Employment Information (On Board Date, Hire Date, Position information), and Education Information.

The Payroll ID is an identifier for our present system and is generated from Time and Attendance (TAA).

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

Identity theft: This system is locked down by permissions only and no one has access to PII except for a few high level personnel with an official need to know. Upon entry, a banner identifies a Privacy Act Statement notifying individuals that the system contains PII information and it is their responsibility to maintain and safeguard.

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.

Yes, however if the individual chooses not to provide the information no record of training or qualification standards can be generated. This could impact the individual's ability to perform hi/her assigned duties and in some cases, it may be impossible for the person to perform assigned duties.

(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.

If personal information is not provided, individual training records could not be maintained.

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.

PAS information is provided to individuals when the data is collected. Upon entry to EC/TMS system a banner with the PAS is provided and terms and conditions statement must be selected before access to the system is initiated.

PRIVACY SENSITIVE FOR OFFICIAL USE ONLY F00R THOSE WITH AN OFFICIAL NEED TO KNOW, UNAUTHORIZED DISCLOSURE OF THIS INFORMTIN MY SUBJECT YOUTO CIVIL OR CRIMINAL PROSECUTION AND PENALTIES.

The Privacy Act of 1974 is a means to regulate the collection, use, and safeguarding of personal data. Privacy Act information is personal data such as a person's social security number, address, or other unique information. These types of data should not be collected without authorization and should not be distributed or released unless the receiver has an official need-to-know.

Privacy Act Statement
Authority: The Government Employees Training Act of 1958 (USC, Title 5, 4104 to 4118), E.O. 9397, November 1943 (SSN)
Purpose: The primary purpose of the information collected is for use in the administration of the Federal Training Program (FTP) to document the nomination of trainees and completion of training. In additional, it serves as the principle repository of personal fiscal and administrative information about trainees and the programs in which they participate. The information becomes a part of the permanent employment record of participants in training programs, and should be included in the Government's Central Personnel Data File.

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.