



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

TRAINING AND OPERATIONAL READINESS INFORMATION SERVICE (TORIS)

Department of the Navy - COMPACFLT - AFLOATRAGRUPAC, N00T-1

### 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  
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.

The Commander Afloat Training Group Pacific (ATGPAC) is the system owner for the TORIS Enterprise. The ATG Enterprise Personnel Program (AEPP) is the subsystem of TORIS that enables collection and tracking of information on all ATG personnel.

TORIS Enterprise collects Name, Gender, Race/Ethnicity, Birth Date, Rank/Rate, Mailing/Home Address, Personal Cell Phone Number, Home Telephone Number, Security Clearance, Spouse Information: Name, Recall; Child Information: children's first names; qualifications, Projected Rotation Date (PRD), Next of Kin (NOK), Emergency Contact Information.

Information is collected on all employees of Afloat Training Group Pacific (ATGPAC), Afloat Training Group Atlantic (ATGLANT), Afloat Training Group West Pacific (ATGWP), Afloat Training Group Middle Pacific (ATGMP), Afloat Training Group Mayport (ATGMayport), and Afloat Training Group Pacific Northwest (ATGNW).

The information is input by Administrative staff when new personnel check-in to the activity. The information is not shared with any other component IT systems.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.). There are risks that TORIS, 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. SSNs are specifically excluded from the TORIS Database. Since TORIS 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 also vulnerable to "insider threats". TORIS managers are vigilant to this threat and limit 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 the system. These individuals have gone through 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.

TORIS does not share any identifiable information outside of the TORIS infrastructure: Name, rank/rate, and qualification is available for designated personnel across the Afloat Training Group to support resource allocation for training events.

**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.

(2) If "No," state the reason why individuals cannot object.

The minimum personnel data must be entered (name, rank/rate, qualification, PRD) in order to provide resource data to command schedulers, who assign trainer personnel to support specific training missions. Individuals are informed during check-in that they can choose not to provide some of the information requested (home address, emergency contact, NOK).

**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.

The minimum personnel data must be entered (name, rank/rate, qualification, PRD) in order to provide resource data to command schedulers, who assign trainer personnel to support specific training missions.

Individuals are informed during check-in that they can choose not to provide some of the information requested (home address, emergency contact, NOK).

**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 PII information is collected during the personnel check-in process from the individual and entered manually into the TORIS database by an administrator. The individual checking in is provided with 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.**