



PRIVACY IMPACT ASSESSMENT (PIA)

For the

TeamMate

Department of the Navy - DON/AA - NAVAUDSVC

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

Not required. PII is not collected directly from any individual.

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.

GAO—12-331G, Government Auditing Standards of December 2011
Inspector General Act of 1978, 5 U.S.C. App 3, as amended
110 STAT 186, Public Law 104-106, National Defense Authorization Act of Feb. 10, 1996
DFARS 237.270, Acquisition of Audit Services

SECNAV INSTRUCTION 7510.7G (Department of the Navy Internal Audit)

ENCLOSURE 5 - Paragraph 1 (Access To Information)

Access to Information. Consistent with the auditors' security clearances, unless access is precluded or limited by law, regulation, or DoD policy, DON auditors must be granted full and unrestricted access to all personnel, facilities, records, reports, databases, documents, or other DON information or material requested, that the Auditor General deems necessary to accomplish an announced audit objective (reference (b)). Such access will be unrestricted and unfettered by burdensome administrative requirements or screening procedures beyond those required by security regulations. All DON personnel shall respond to any request or inquiry by the Auditor General of the Navy within the scope of the audit function, as if made by the Secretary of the Navy. Per reference (b), all access granted, or information or material provided to the audit organizations will be on a nonreimbursable basis. Within the DON, this includes property or services provided, automated data processing support, data retrieval, and programming, as needed, to perform the audit. The Naval Audit Service will retain possession and

determine the disposition of all audit documentation.

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.

TeamMate is an electronic audit work paper application package that supports the automation of the audit work paper process, including preparation, review, reporting, and tracking. The application never retrieves records using a personal identifier or any other mechanism.

PII collected is all unstructured information and could be any PII element.

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

Administrative: Access to TeamMate is controlled by NMCI network access authentication (i.e., Common Access Card) and project assignment (permission request form); permission assignment is performed by the NAVAUDSVC TeamMate Specialist. TeamMate users' permissions are restricted to their specifically assigned project. NAVAUDSVC TeamMate administrators have full administrative access to all projects.

Technical: TeamMate data are stored within the application itself. There is no central database repository. End users use the TeamMate application which is locally installed on their desktop. Access to TeamMate is controlled by NMCI network access authentication (i.e., Common Access Card), project assignment (permission request), and permission assignment is performed by the NAVAUDSVC TeamMate Specialist.

Physical: All personnel entering the building must have appropriate identification; visitors are escorted. All users must authenticate to the NMCI network using their Common Access Card (CAC).

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.

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

PII is not collected from individuals directly. All supporting audit data files that include PII are received from the command/agency being audited.

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.

PII is not collected from individuals directly. All supporting audit data files that include PII are received from the command/agency being audited.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

PII is not collected from individuals directly. All supporting audit data files that include PII are received from the command/agency being audited.

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.