



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Automated Neuropsychological Assessment Metrics (ANAM)

Department of the Navy - TMA DHP Funded System

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.

System of Record Authorities: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 1095, Collection from Third Party Payers Act; 10 U.S.C. 5131 (as amended); 10 U.S.C. 5132; 44 U.S.C. 3101; 10 CFR part 20, Standards for Protection Against Radiation; and, E.O. 9397 (SSN), as amended

Medical and dental care in the DoD are authorized by Chapter 55 of Title 10 U.S.C., section 1071 - 1106.

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.

ANAM is a proven Army computer-based tool that is being deployed DoD-wide that is designed to detect a service member's speed and accuracy of attention, memory, and thinking ability. By using a pre-deployment test, a baseline is established in the event that the Service Member becomes injured or is exposed to a traumatic brain injury (TBI). If the Service member is injured then they will take another test and the results are compared to their original baseline to determine what would be the best course of treatment or care. This comparison will help determine the extent of the injury in a more efficient manner.

It does not diagnose any medical condition. ANAM pre-deployment testing is not a diagnostic tool and is not used to determine if the Service Member is deployable or non-deployable.

On May 28, 2008 The Assistant Secretary of Defense, Health Affairs office released a memorandum directing all Services to begin implementing baseline pre-deployment neurocognitive assessments for all service members. All services members are required to complete their pre-deployment neurocognitive assessment within 12 months prior to deployment. This assessment is a mandatory requirement for deployment.

Name, SSN, gender, birth date, personal cell phone number, home address, unit information, deployment operation, administration site, and reason for assessment are collected to associate the test results with the individual service member. The assessment results will be securely stored electronically in accordance with the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

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

All systems are vulnerable to "insider threats." MTF information managers are vigilant to this threat by limiting 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 ANAM. These individuals have gone through DoD background and employment investigations. The ANAM system employs security in multiple ways: Physical access to the ANAM hardware, operating systems, application software, electronic media, and all other system components is controlled through defense-in-depth security methods. There is a combination of electronic locks, security personnel, video cameras, and monitoring devices that monitor and control physical access. Only privileged users can access ANAM.

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. The authorized ANAM proctors, both government employees and contractors, will have access to PII as part of their duties.

Other DoD Components.

Specify. U.S. Army ANAM Office. The ANAM Office owns the data repository for ANAM data and is responsible for providing the data service wide for reporting.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

EYAK Development Corporation. The contract contains business associate agreement language and the contractor agrees to abide by all HIPAA Privacy and Security requirements regarding health information as defined in this clause and in DoD 6025.18-R and DoD 8580.02-R. The contractors are under a U.S Army contract and are sent to the facilities where they provide all services including test proctoring and handling the data.

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.

Participation is mandatory prior to deployment.

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.

[Empty rectangular box]

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

The individual's PII is required to correlate pre and post deployment data.

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.

During the briefing prior to taking the test the individual is briefed on the Privacy Act.
When the individual logs into the laptop to start the test a flash screen gives a Privacy Act advisory.

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.