PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Automated Neurocognitive Assessment Metrics (ANAM)
UNITED STATES AIR FORCE

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 DHA 07, Military Health Information System (March 30, 2006).

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.

5 U.S.C. 301, Department Regulation; 10 U.S.C., Chapter 55; Pub.L. 104-91, Health Insurance Portability and Accountability Act of 1996; DoD 6025.18-R, DoD Health Information Privacy Regulation; 10 U.S.C. 1071-1085, Medical and Dental Care; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b, TRICARE Prime and TRICARE Program; 10 U.S. C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD 6010.8-R, CHAMPUS; 10 U.S.C. 1095, Collection from Third Party Payers Act; and E.O. 9397 (SSN).

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.

Traumatic brain injury (TBI) is a high profile injury from the current conflicts in Iraq and Afghanistan. As a result of recommendations from several reports, the Office of the Deputy Assistant Secretary of Defense (Force Health Protection and Readiness) was given the lead for strategic TBI and PTSD planning. Neurocognitive assessment in the evaluation of TBI is an important element in the overall force health protection strategy.

Concussion/mild TBI (mTBI) has been a special area of concern. By current definitions, concussion/mTBI can range from a brief alteration of consciousness with rapidly resolving symptoms to loss of consciousness up to 30 minutes and posttraumatic amnesia for up to 24 hours. Assessing individuals following concussion/ mTBI with respect to appropriate management and return to duty (RTD) decisions is a crucial factor driving the need for pre-deployment baseline cognitive testing. This testing is based on the assumption that having baseline information would be of more benefit than relying exclusively on military norms when evaluating a Service Member (SM) post-injury in the field who has been diagnosed and for whom RTD is being considered. The purpose of these implementation guidelines is to insure the consistency and integrity of the baseline process understanding the goal of the program is to provide data to clinician's in-theater to facilitate their clinical and RTD assessments.

The current NCAT is the Automated Neuropsychological Assessment Metrics (ANAM) test system. ANAM is the identified tool to be used for pre-deployment baseline testing while research continues to evaluate various computerized neurocognitive test options. ANAM is a tool developed within DoD with funding by the US Army. The full ANAM test system includes a library of over 30 tests that assess different cognitive domains and which can be used to build specific batteries to address different clinical conditions. The 20-minute ANAM4 TBI battery is composed of specific ANAM tests that have been used in multiple clinical studies including studies of concussion and traumatic brain injury. The report generated by this system makes use of baseline data when available but can also be used to compare a SM's test performance against extensive military norms.

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

The data is currently being collected on devices that are not connected to any network. Information is encrypted using an approved DoD tool prior to storage or transfer. Access is limited to those with the need to know while keeping the information secure from those who do not.

Coordination of four discreet potential privacy risks is being incorporated in implementing ANAM:

- Unauthorized access
- Inaccurate information
- Privacy and due process right protection
- Unauthorized disclosure

In response to the risk of unauthorized access to the sensitive information that records within ANAM will contain, warning banners and Privacy Act statements in accordance with DoD regulations. Physical safeguards (e.g., data stored on accredited servers), technical safeguards (e.g., encryption; common access card, password protection) and procedural safeguards (e.g., physical access to data based on duty position) are employed in series to ensure only those personnel that demonstrate "need to know" can access information contained within ANAM. In response to the risk presented by including inaccurate information in the system, ANAM correlates information from authoritative sources only. In addition to the Freedom of Information Act (FOIA) request process, the system allows users to report inaccurate information on their records. In response to the risk of violating the rights of the individuals involved in the medical process, the Air Force is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. Data is only viewed by selected ANAM users and medical personnel that require access to the information in the performance of their duties. In response to the risk

of unauthorized disclosure of information contained; the program requires that users receive information assurance awareness, HIPAA, and the Privacy Act, and system training in order to mitigate risks involved. This multi-faceted approach to safeguarding PII provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

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. ANAM data sharing (in identifiable form) is specifically for military health care providers to aid in the treatment/care of Service Members. The intent is to share the results with medical staff responsible for patient care and also ANAM data sharing (in identifiable form) is specifically for military healthcare providers to aid in the treatment/care of service members. To ensure sensitive data is protected, the data-at-rest (DAR) solution for ANAN is Credant-2-go; however the way-ahead is migration to Guardian Edge.

☒ **Other DoD Components.**

Specify. The ANAM data may be shared with the medical staff at Army, Navy, or Marine to facilitate treatment/care of Service Members. The intent is to jointly share the results with Tri-Service medical staff responsible for patient care. ANAM data sharing (in identifiable form) is specifically for military healthcare providers to aid in the treatment/care of service members. The intent is to jointly share the results with tri-service clinicians responsible for patient care.

☒ **Other Federal Agencies.**

Specify. ANAM data may be shared with the Veterans Affairs to assist in continuing treatment/care of Service Members after separation from the Service.

☐ **State and Local Agencies.**

Specify.

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

Specify. Eyak Development Corporation. HIPAA Business Associate Language, approved by the TRICARE Management Activity Privacy Office, is included in the current contract between EDC and the Office of the Surgeon General, Army.

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

Specify. ANAM data may be shared with medical providers to assist in continuing treatment/care of Service Members after separation from the Service.

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.

The Service Members are provided a verbal briefing prior to the assessment and Service Members may choose object to the collection of PII. All PII collected during the assessment are provided by Service Members.

(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.

ANAM data is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and DoD 6025.18-R, DoD Health Information Privacy Regulation'. Service Members who wishes to give or withhold their consent should contact the AF HIPAA Privacy Officer or the Privacy Act Office.

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

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 system screen, educational materials and flyers prominently displays the system HIPAA Privacy DoD Information Systems Security notices in accordance with the law and DoD policy. Individuals are verbally briefed on the ANAM assessment process. No identifiable data will be provided to an individual. Health care providers may access this data as they evaluate 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.

Privacy

Privacy

Privacy

Privacy

Privacy

Privacy

Privacy

Privacy

Privacy