PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Institutional Review Board (EIRB)
Military Health System (MHS) / TRICARE Management Activity (TMA)

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 18

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 0720-0042

Enter Expiration Date 12/31/2013

☐ **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.

32 CFR 219.115, Protection of Human Subjects and DoDD 3216.02, 4.5 and 5.3, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research," March 25, 2002.

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 mission of the human research protection program is to foster and oversee research and development activities by promoting policies and procedures that facilitate timely and effective reviews of research and ensuring that approved research is conducted in accordance with applicable rules and ethical guidelines to protect the rights and welfare of the participants, including service members, employees, and their families. The purpose of this system is to track individual researchers to ensure that everyone engaged in the performance of research at the DoD member institutions is properly trained and qualified.

Personally identifiable information (PII) that may be collected include:
Name
Address
Phone numbers
Personal E-mail address
Employment information
Education information

Information will be collected from and about any category of individuals that uses this system to submit a research proposal.

According to DoD Directive 3216.02, the Under Secretary of Defense for Personnel and Readiness has delegated responsibilities with respect to matters affecting medical research to the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). Therefore, the system is centrally managed and owned by HA.

System POC:
Program Manager, Research Regulatory Oversight
5113 Leesburg Pike
Suite 901
Falls Church, VA 22041

The system will be accessed by all participating sites. The system is accessible to the public via the web; however, investigators will only have access to their own information.

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

Potential mishandling of PII is low. The privacy risks associated with the PII collected are unauthorized access, inaccurate information entered into the application/form, and unauthorized disclosure of PII.

Safeguards:
Force Health Protection and Readiness (FHP&R) has a mandatory requirement, tracked by itself, for all individuals to complete Department of Defense (DoD) Information Assurance (IA) training as well as Privacy Act training. System access is monitored by system administrators and routinely checked for requirements of access. All users of the system are required to justify their access via their supervisor. Security Safeguards are in place to mitigate the risks.

A dedicated IA team addresses security posture of data center and the application that resides within. As a result the application and its supporting database are being built/maintained to Defense Information Systems Agency (DISA) standard Security Technical Information Guides (STIG) requirements. The application is hosted in a secure, access controlled facility, and staffed with experienced system administrators and IA personnel who have the appropriate security clearances. All personnel, including contractors and vendor personnel, are required to obtain and maintain FHP&R security badges, Common Access Cards (CAC), Army Knowledge Online (AKO)/Defense Knowledge Online (DKO) accounts and to adhere to the security requirements of the FHP&R data center secured facility. Access to servers is provided on a need-to-know basis and to authorized authenticated personnel only. Defense-in-depth security layers, including but not limited to, Firewall, Host Bases Security System (HBSS), Intrusion Detection System

(IDS), Access Control Lists, Secure Socket Layers (SSL) such as Hypertext Transfer Protocol Secure (HTTPS) and, CAC and password authentication, are in place to protect the software application, back end database and associated systems. Records are maintained in a secured area. Password authorization and monitoring are the responsibility of the system managers.

The system provides two-factor DoD authentication from any site including CAC and passwords, by leveraging Single Sign-On capabilities via AKO/DKO. Access to personal information is restricted to those who require the data in the performance of the official duties, and have received proper training relative to the Privacy Act and Information Assurance.

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. OUSD(P&R) Research Regulatory Oversight Office personnel located at the following institutions:

Uniformed Services University of the Health Sciences (USUHS)
HA/TMA (includes DCoE)
Defense Human Resources Activity
Department of Defense Education Activity
Defense Equal Opportunity Management Institute
Reserve Affairs
Military Community and Family Policy

☒ **Other DoD Components.**

Specify. Army, Navy, and Air Force representatives

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Booz Allen Hamilton, Henry M. Jackson Foundation and other organizations that provide on-site review support to the DoD human research protection program.
All contracts contain language which require the contractor to comply with the Privacy Act of 1974, as amended.

☐ **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.

Individuals can object by not submitting requests for approval to engage in or to conduct research. The

submission of PII in the system is voluntary. However, failure to provide the PII will result in the individual not being able to conduct research at any of the member DoD institutions.

(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.

PII is collected in the system to permit identification, tracking and oversight of authorized research procedures and to track the individual researchers and reviewers involved in the process. The purpose of tracking individuals is to ensure that everyone engaged in the performance or oversight of research is properly trained and qualified. PII is only used and disclosed as outlined in the Privacy Act System of Record Notice (SORN) published in the Federal Register.

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

The following Privacy Act Statement appears within the system prior to the point of collection:

format.

AUTHORITY: 32 CFR 219.115, Protection of Human Subjects and DoDD 3216.02, 4.5 and 5.3, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research," March 25, 2002.

PURPOSE: The data is collected to maintain a case file for use by defense research oversight offices concerning any research protocol. The purpose of tracking individuals is to ensure that individuals engaged in the performance or oversight of research is properly trained and qualified.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, the DoD "Blanket Routine uses" under 5 U.S.C. 552a(b)(3) apply to this collection. Information from this system may be used for identification, tracking and oversight of authorized research procedures and to track the individual researchers and reviewers involved in the process and may be shared with federal, state, local, or foreign government agencies, and to private business entities, including on matters relating to eligibility, quality assurance, peer review, program integrity, and civil or criminal litigation.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in you not being eligible for the position.

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.