PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Blood Standard System (DBSS)
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: 135
- ☐ **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 007-97-01-15-02-0567-00

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

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	DoD Clearance and OMB Licensing requirements are currently being reviewed by the TMA Information Collection Management Officer. The PIA will be updated accordingly with their decision.
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, as follows: a) 10 U.S.C. §§ 1071-1085 (Medical and Dental Care); b) 10 U.S.C. §§ 1097a and 1097b (TRICARE Prime and TRICARE Program); c) 10 U.S.C. § 1079 (Contracts for Medical Care for Spouses and Children); d) 10 U.S.C. § 1079a (CHAMPUS: Treatment of funds and other amounts collected); e) 10 U.S.C. § 1086 (Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents); and, f) 10 U.S.C. § 1095 (Collection from Third Party Payers Act); 42 U.S.C. §§ 11131-11152 (Reporting of Information); 45 C.F.R. §§ 160 and 164, Parts A and E (Health Insurance Portability and Accountability Act of 1996); DoD 6025.18-R (DoD Health Information Privacy Regulation); DoD Instruction 6015.23 (Delivery of Healthcare at Military Treatment Facilities); DoD 6010.8-R (CHAMPUS); DoDI 6480.4 (Armed Services Blood Program (ASBP) Operational Procedures) DoDD 6000.12 (Health Services Operations and Readiness); 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.

Defense Blood Standard System (DBSS) is a Food and Drug Administration (FDA) regulated Class II Medical Device designed to handle blood collection, processing and tracking procedures, and automation of standards and safeguards of the Military Health System (MHS). DBSS supports the Armed Services Blood Program (ASBP), which represents the Army, Navy, and Air Force by providing high quality blood products and services to 9.1 million MHS beneficiaries as an element of national policy in peacetime and during deployed operations. The DBSS Program Office provides application support and maintenance while the individual services maintain licenses to control all patient data has ultimate responsibility to maintain and ensure compliance with the security and privacy policies.

DBSS mitigates the risk to beneficiaries of transfusion-transmitted infectious diseases. DBSS currently is used at blood donor and transfusion centers in peacetime military facilities. DBSS reduces risk of infectious disease transmission by identifying ineligible blood donors prior to blood collection. DBSS further reduces risk by quarantining blood products that contain infectious agents and by implementing automated critical control checkpoints throughout the entire process of donating, testing, labeling, shipping, and transfusing blood products. By using management reports, DBSS provides field commanders an accurate, real-time picture of the available blood supply.

Personally identifiable information collected by the system includes: Name, Social Security Number, date of birth, gender, address, phone number and medical information.

DBSS has a bi-directional interface to Composite Health Care System (CHCS) and has an out bound uni-directional interface to the Joint Medical Asset Repository (JMAR). JMAR does not contain PII. DBSS is classified as mission-essential, sensitive, and DoD Mission Assurance Category (MAC) II.

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

Blood donation is a voluntary process. Any potential privacy risks associated with the PII collected have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of data.

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. Composite Health Care System (CHCS), Defense Enrollment and Eligibility Reporting System (DEERS)

☐ **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. 5D Information Management Inc.

Contractors provide support for DBSS for approximately 75 DoD sites. This support includes direct support to the sites, configuration management of the application, and the storage of historical data. Data Use Agreements (DUAs) are in place to control, monitor, and enforce compliance with Federal laws and DoD regulations related to the release of PHI to internal and external requestors.

☐ **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.

Blood donation is a voluntary process; as such the collection of information is voluntary.

(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.

Blood donation is a voluntary process; as such the collection of information is voluntary. Individuals have the opportunity to authorize the use of their PII/protected health information (PHI) by signing DD Form 572, Blood Donation Record.

(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.

DD Form 572

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.