PRIVACY IMPACT ASSESSMENT (PIA)

For the

Blood Management Blood Bank/Transfusion Service (BMBB/TS)
Defense Health Agency (DHA)

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: 13520 (EBMS)
- ☐ **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 UII: 007-000003993 (EBMS)

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 EDHA 07, pending new BMBB/TS SORN publication.

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	BMBB/TS is in process of obtaining an 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.

10 U.S.C., Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities; and E.O. 9397 (SSN), as amended.

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 purpose of the Blood Management Blood Bank Transfusion Service (BMBB/TS) will manage the blood transfusion aspect of the Armed Services Blood Program (ASBP), including blood records, blood orders, and transfusion patient information in the Continental United States (CONUS) and Outside Continental United States (OCONUS). BMBB/TS will manage the Military Treatment Facility (MTF) inpatient and outpatient blood test results for transfusion compatibility.

BMBB/TS is part of the Enterprise Blood Management System (EBMS) initiative which will employ two separate and distinct FDA regulated Class II Medical Devices – Blood Donor Management System (BDMS) and the Blood Management Blood Bank/Transfusion System (BMBB/TS) – providing an effective "arm-to arm" solution. BDMS and BMBB/TS will replace the current legacy system, the Defense Blood Standard System (DBSS).

The main purpose of BMBB/TS is to provide the following high-level functionality:

• Automate operations while giving MTF staff the control needed to manage specimens, orders, blood products, derivatives, and routine and electronic cross-matching

• Manage supply to meet demand with an easy-to-use inventory overview screen with real-time updates

• Track patient history and raise the bar on patient safety with over 60 built-in checks and real-time patient monitoring to pro-actively alert staff of potential errors

The types of personal information about individuals that will be transcribed/maintained in the BMBB/TS system include personal descriptors, unique identification numbers, health information, and ethnicity information.

BMBB/TS will be accessible by authorized users (i.e., government civilians, military government contractors, and other contract support) from 62 Military Treatment Facilities (MTFs). The system hosts a web application that will not be accessible by the public; rather, it will be restricted to authorized users.

BMBB/TS is owned and managed by Defense Health Clinical System (DHCS), which is a Military Health System (MHS) /Defense Health Agency (DHA) Program Office. The Commercial off the Shelf (COTS) medical device manufacturer is Mediware Information Systems, Inc.

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

All applicable security and privacy processes and regulations (e.g., the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Privacy Act of 1974, as amended, etc.) have been defined and implemented, reducing privacy risks to the maximum extent possible.

The central computing network center housing the BMBB/TS application and network communication servers have comprehensive physical, technical, and administrative controls, in accordance with Department of Defense (DoD) 8580.02-R, "DoD Health Information Security Regulation". Office door locks, password enabled screen savers, monitoring by facility staff, application time-outs, and BMBB/TS technical controls that prevent unauthorized individuals from logging onto the system provide protection for PII / PHI stored in BMBB/TS.

The system architecture security requirement ensures that the system security safeguards are protected from access, modification, and destruction by unauthorized personnel.

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) and MTF Occupational Health Departments (in order to disclose to military personnel and beneficiaries test results)

☐ **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. -Kratos Technology & Training Solutions

-Planned Systems International (PSI), Inc.

-Mediware Information Systems, Inc.

The following language is contained in all contracts and sub-contracts awarded by the government: "The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The contractor shall also comply with federal laws relating to freedom of information and records management.

Under DoD 6025.18-R, "DoD Health Information Privacy Program," January 24, 2003, reasonable steps must be taken to implement appropriate procedural, administrative, technical and physical safeguards to prevent the unauthorized use and/or disclosure of any personally identifiable information (PII) or PHI. Likewise, all uses, disclosures, and destruction of PII and PHI data are generally subject to DoD 5400.11-R, "DoD Privacy Program," May 14, 2007 and DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007."

☐ **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.

BMBB/TS is not the initial point of collection of PII / PHI from individuals/patients; therefore, patients do not have the opportunity to object to the collection of their PII / PHI. The patient initial point of collection is not conducted in the Blood Bank/Transfusion Services department. The initial point of PII collection is CHCS / AHLTA. The initial point of collection for PHI is the clinical laboratory phlebotomy section or different Military Treatment Facility (MTF) departments (in-patient, emergency room, urgent care, etc...) where the blood sample is collected/drawn from the in-patient/out-patient. This information is required to correctly identifying the patient both during collection of the pre-transfusion sample and before starting the transfusion.

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.

BMBB/TS is not the initial point of collection of PII / PHI from individuals/patients; therefore, patients do not have the opportunity to object to the collection of their PII / PHI. The patient initial point of collection is not conducted in the Blood Bank/Transfusion Services department. The initial point of PII collection is CHCS / AHLTA. The initial point of collection for PHI is the clinical laboratory phlebotomy section or different Military Treatment Facility (MTF) departments (in-patient, emergency room, urgent care, etc...) where the blood sample is collected/drawn from the in-patient/out-patient. This information is required to correctly identifying the patient both during collection of the pre-transfusion sample and before starting the transfusion.

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 | BMBB/TS does not collect personally identifiable information (PII) directly from individuals. Therefore, no Privacy Act Statement or Privacy Advisory is required. The PII contained in BMBB/TS

applicable format.	is collected by the Composite Health Care System and AHLTA. PII is collected at the laboratory phlebotomy section or military treatment facility where the blood sample is collected/drawn from the in-patient or out-patient. The Transfusion Services Technician then performs verification checks and cross matching on the blood sample before sending the blood sample to its final destination for transfusion.

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.