PRIVACY IMPACT ASSESSMENT (PIA)

For the

Blood Management Blood Bank/Transfusion System (BMBB/TS)
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	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 007-97-01-17-02-3993-00 (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 DHA 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	An OMB Control Number is in process for BMBB/TS
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; DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD 6010.8-R, CHAMPUS; 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.

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.

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), Outside Continental United States (OCONUS), and in Theater. BDMS and BMBB/TS will replace the current legacy system, the Defense Blood Standard System (DBSS).

The main purpose of BMBB/TS is to manage Military Treatment Facility (MTF) inpatient and outpatient blood test results for transfusion compatibility.

BMBB/TS will 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; and

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

BMBB/TS may collect the following personally identifiable information (PII) / protected health information (PHI):

• Name
• Other Names Used (Alias)
• Truncated Social Security Number (SSN)
• Other ID Number (Electronic Data Interchange Personal Identifier (EDIPN) – planned incorporation)
• Gender
• Race / ethnicity
• Birth date
• Medical information

BMBB/TS is currently in the Engineering and Manufacturing Development and Demonstration phase; this system is owned and managed by Defense Health Information Health Management System (DHIMS), which is a Military Health System (MHS) / TRICARE Management Activity (TMA) Program Office. The Commercial off the Shelf (COTS) medical device manufacturer is Mediware Information Systems, Inc.

BMBB/TS POC:
DHIMS
5109 Leesburg Pike
Falls Church, VA 22041
(703) 998 - 6900

(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" for MAC II Sensitive systems. 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); Armed Forces Health Longitudinal Technology Application (AHLTA); MTF Occupational Health Departments (in order to disclose to military personnel 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.

Thundercat Technology, LLC
1775 Wiehle Ave. Suite 101
Reston, VA 20190

Planned Systems International (PSI), Inc.
10632 Little Patuxent Parkway, Suite 200
Columbia MD, 21044

Mediware Information Systems, Inc.
11711 West 79th St.
Lenexa, KS 66214

TechWerks, LLC
552 Desert Oak Dr.
Pensacola, FL 32514

Akimeka
1305 N. Holopono St., Ste. 3
Kihei, HI 96753

The following language is contained in all contracts and sub-contracts awarded by the government:

"The TMA Privacy Office website at http://www.tricare.mil/tmaprivacy/contract.cfm contains guidance regarding Protected Health Information (PHI) and Personally

Identifiable Information (PII). The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data.

The Contractor shall ensure that data which contains PHI is continuously protected from unauthorized access, use, modification, or disclosure. Contractor shall comply with all previously stated requirements for HIPAA, Personnel Security, Electronic Security, and Physical Security."

☐ **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; therefore, individuals do not have the opportunity to object to the collection of their PII / PHI.

The initial point of PII collection is CHCS / AHLTA. The initial point of collection for PHI is the clinical laboratory or ward where blood is drawn.

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; therefore individuals do not have the opportunity to consent to the specific uses of their PII / PHI.

The initial point of PII collection is CHCS / AHLTA. The initial point of collection for PHI is the clinical laboratory or ward where blood is drawn.

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.

BMBB/TS is not the initial point of collection of PII / PHI from individuals; therefore no privacy act statement or privacy advisory is given to individuals for this system.

The initial point of PII collection is CHCS / AHLTA. The initial point of collection for PHI is the clinical laboratory or ward where blood is drawn.

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.