PRIVACY IMPACT ASSESSMENT (PIA)

For the

Business Common Services/BusinessObjects XI (BCS/BOXI)
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

☐ **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 EDHA 07; EDTMA 04; EDHA 16

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.

• M2: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); and E.O. 9397 (SSN), as amended.

• PEPR systems: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

• SNPMIS draft revision: 10 U.S.C. Chapter 55, Medical and Dental Care; 20 U.S.C. 921, Defense Dependents' Education System; 20 U.S.C. Chapter 33, Education of Individuals With Disabilities; DoD Instruction 1342.12, Provision of Early Intervention and Special Education Services to Eligible DoD Dependents; and E.O. 9397 (SSN), as amended.

• TED: 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (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.

BCS/BOXI is a Business Intelligence platform where DHSS reporting and analytical needs are served at the departmental or enterprise level. The system provides a set of tools and interfaces to developers and end-users to create reports and analyze their data eliminating the need to master the underlying complexity of the data relationships. BCS/BOXI is providing reporting and analytical services to the user communities of the Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2), Expense Assignment System IV (EAS IV), Special Needs Program Management Information System (SNPMIS), TRICARE Encounter Data (TED) and Patient Encounter Processing and Reporting (PEPR) systems. Administrators maintain the system. Developers design/develop universes and reports available for end users to use. End-users refresh reports developed by developers or develop their own ad hoc reports.

BCS/BOXI is in its Operations and Support system life cycle phase. DHA owns and operates BCS/BOXI. BCS/BOXI has been designated as a Mission Assurance Category (MAC) III, Sensitive system as defined by DoD regulations. BCS/BOXI provides reporting functionality that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness.

The system is accessible via a public web site across the internet by anyone with the Uniform Resource Locator (URL). BCS/BOXI is a Public Key Infrastructure (PKI) authentication enabled application. No external user can gain access to neither the BOXI application nor the environment unless they have a Common Access Card (CAC) that is successfully authenticated and the Electronic Data Interchange Personal Identifier (EDIPI) on the authenticated CAC has been set-up and authorized on the enterprise Lightweight Directory Access Protocol (LDAP) to allow access to the BusinessObjects shared services environment.

BCS/BOXI users may generate reports that include PII information such as name, social security number, race/ethnicity, birth date, and much more. Each user can only create reports of information for the source systems that they have access to and the PII is not consistent across all systems that connect to BOXI. BOXI users from M2 may be able to create reports of PII that is different from what BOXI users from EAS IV can create reports from.

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

The privacy risks associated with PII/PHI collected is the risk of disclosure when users fail to lock their workstations when not in use or a hacker breaking into the system and stealing the PII/PHI. These risks are mitigated through the implementation of various administrative, technical and physical security controls, such as the use of CAC, use of Secure Sockets Layer to access BCS/BOXI environment, implementation of Role-based access control within the application, and security awareness training requirement. Risks regarding the collection, use and sharing of PII/PHI in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls. Also, system users are required to submit an Account Authorization Request Form (AARF) and have the need for access validated.

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. DHA (Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2), Expense Assignment System IV (EAS IV), Special Needs

Program Management Information System (SNPMIS), TRICARE Encounter Data (TED) and Patient Encounter Processing and Reporting (PEPR) systems)

☐ **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.

☐ **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.

This systems collects PII and PHI from Patient Encounter Processing and Reporting (PEPR), TRICARE Encounter Data (TED), Expense Assignment System IV (EAS IV), Special Needs Program Management Information System (SNPMIS), and Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2).

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.

This systems collects PII and PHI from Patient Encounter Processing and Reporting (PEPR), TRICARE Encounter Data (TED), Expense Assignment System IV (EAS IV), Special Needs Program Management Information System (SNPMIS), and Military Health System (MHS) Management Analysis and Reporting Tool (MART) (M2).

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.

Although BCS/BOXI is a SOR, it does not collect PII directly from individuals. Rather, BCS/BOXI is a SOR because of how it retrieves PII received from source SORs which collect directly from individuals. As such, a Privacy Act Statement is not necessary in connection with BCS/BOXI.

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.