PRIVACY IMPACT ASSESSMENT (PIA)

For the

Benchmark Tracker (BMT) Online Assessment Delivery System
Department of Defense Education Activity

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 DoDEA 26

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.

DoDEA 26;
10 U.S.C. 113, Secretary of Defense;
10 U.S.C. 2164, Department of Defense Domestic Dependent Elementary and Secondary Schools;
20 U.S.C. 921-932, Overseas Defense Dependent's Education;
29 U.S.C. 794, Nondiscrimination under Federal Grants and Programs;
DoD Directive 1342.20, Department of Defense Education Activity (DoDEA);
DoD Directive 1020.1, Nondiscrimination on the Basis of Handicap in Programs and Activities Conducted by the Department of Defense;
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 system is to (1) provide an online testing platform for the delivery of the DoDEA U.S. History End-of-Course Assessment and (2) maintain a record of students who have taken the DoDEA U.S. History EOC Assessment and the student performance. The system is organized into 3 sections: Classes, Assessments, and Reports. Teachers, school administrators, and above-school level personnel on the district, area and HQ level can view student and class data. Personal information collected in the system includes student first and last name, student ID #, gender, date of birth, race/ethnicity, English Language Learner (ELL), and Special Education Services.

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

Privacy risks are minimized because of the following factors:
(1) A username and password is required to access the online data management system:
All hosts and network devices are configured to use central logging servers running a commercial log management system (Splunk). All security events are routed through these logging servers with appropriate notifications (both e-mail and SMS) configured to notify Bookette IT staff 24/7 in-case of emergency.
All devices are monitored using SNMP monitoring servers and have very careful thresholds defined to detect anomalous situations such as a sudden spike in network or CPU usage.

(2) Information in the online data management system is restricted to those stakeholders given access on a hierarchical level; DoDEA area, district, school, and class.

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.

☐ **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.

Pearson:
5.8 Security: The Contractor shall provide a secure, encrypted FTP site that is (1) capable of selectively limiting and controlling access to online content, resources and backend functions, both internally and externally, for its diverse user community; and (2) provides for the transfer and storage of all assessment items and data. Evidence of digital security shall be supplied by the Contractor.
HE1254-08-C-0008 P00004

Page 9 of 10
All online resources and instructional software shall meet DoDEA information security requirements, such as not containing vulnerabilities posing risk to the network. All software and websites will undergo preliminary testing to ensure that it poses no security risk to the DoDEA Infrastructure. Any IT component of the Contractor's proposal that fails to meet DoDEA's information security and technology requirements will be excluded from further evaluation. All software/Plug-Ins/Add-ons shall be capable of meeting DoDEA's requirements for the DoD Information Assurance Certification & Accreditation Process (DIACAP), Defense Information Systems Agency (DISA) Information Assurance Vulnerability Assessment (IAVA) requirements, and Security Technical Information Guidance (STIG) standards. The contractor shall provide security patches, patch updates, upgrades, and work-a-rounds for software, including 3rd party applications, in response to public released vulnerabilities associated with their software solution. Contractor software solutions shall not interfere with other installed software and shall not modify the system security configuration. The Contractor shall develop and provide software upgrades within 30 days of notification should any of the software/plug-ins be found vulnerable and non-compliant with DISA standards. Software upgrades and patches shall be included in the licensing cost and performed at the least disruptive times. Any additional software requirements may be subject to DIACAP security review prior to contract award.

☐ **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.

PII was collected during the student registration process (DoDEA Form 600). Privacy rights are explained on DoDEA Form 600.

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 was collected during the student registration process (DoDEA Form 600). Privacy rights are explained on DoDEA Form 600.

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.

PII was collected during the student registration process (DoDEA Form 600). The Privacy Act Statement, Authority 10 U.S.C. 2164 and 20 U.S.C. 921, is included on the Student Registration Form 600.

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.