Privacy Impact Assessment (PIA)
for the

National Blue Ribbon Schools Program (BRSP)
March 18, 2022

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Aba S. Kumi/Director, National Blue Ribbon Schools Program
Contact Email: aba.kumi@ed.gov

System Owner

Name/Title: Aba S. Kumi/Director, National Blue Ribbon Schools Program
Principal Office: Office of Communications and Outreach

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The National Blue Ribbon Schools Program (BRSP), a U.S. Department of Education (Department) initiative, recognizes outstanding public and non-public schools. BRSP is a management system consisting of multiple websites and a backend database maintaining a secure data collection. The first BRSP website (https://liaison.nationalblueribbonschools.ed.gov) is used by States and other nominating entities, including Department of Defense Education Activity (DoDEA), Bureau of Indian Education (BIE), and Council for American Private Education (CAPE), to nominate exemplary schools for recognition. The second website (https://portal.nationalblueribbonschools.ed.gov) is used by schools to complete applications for recognition once they have been nominated by a State or other entity. A panel of Federal contractors access the screening portal (https://screening.nationalblueribbonschools.ed.gov) to review applications from nominated schools to ensure they meet the criteria for recognition. Reviewers are able to read, provide comments on, and adjudicate applications through the screening portal. Once schools have been selected for the award, winning schools and their applications are posted on the public-facing website (https://nationalblueribbonschools.ed.gov).

Nominating entities and nominated schools that are completing applications need to register for an account in order to complete the nomination or application process. A representative from the entity may register for an account on the relevant website by providing the required information to the Office of Communications and Outreach (OCO). Data collected include: name of school principal, official school/organizational name, school/organizational mailing address, school/organizational phone number, school/organizational fax number, school/organizational email address, name of district superintendent, and name of school board chairperson. In addition, throughout the application there are open fields for response based on specific questions. These questions are phrased in a way for responses to be general or discussed in aggregate and are not requesting information about specific individuals. All accounts are verified prior to access being granted. School data are collected from States and other nominating entities. Nominated schools also provide information about their specific schools.

Representatives of nominated schools, States, and nominating entities are the only members of the general public that may access BRSP.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

The information collected, used, maintained, and shared by the BRSP system is required as part of the application process to document exemplary schools. The purpose for collecting the name of the school's principal and superintendent is for communication and recognition purposes. All the information requested are in the public domain and easily available and accessible to the public via internet searches.

In addition, information may be collected when individuals use the "Contact Us" page to request assistance or submit questions or issues that are experienced while using the BRSP website.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

The prior PIA was completed on March 21, 2018. This PIA is being updated as part of the regular review process.

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The BRSP is authorized by the Every Student Succeeds Act, Public Law 114–95 (December 10, 2015), Title 1—IMPROVING BASIC PROGRAMS OPERATED BY STATE AND LOCAL EDUCATIONAL AGENCIES. Prior to the Every Student Succeeds Act, the BRSP was authorized by No Child Left Behind Act, Public Law 107-110 (January 8, 2002), Part D—Fund for the Improvement of Education, Subpart 1, Sec. 5411(b)(5).

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

☐ No

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

The information is not retrieved by an identifier. The information within the system is retrieved by school name, by state, and/or by school type.

Records Management

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

ED Records Schedule Number: 102. Recognition Programs Files (ED 102).
Disposition: These are permanent records, cut off annually upon close of program awards cycle, and transferred to NARA after cutoff.
Disposition authority: N1-441-09-6.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

Name of school principal, name of district superintendent, name of school board chairperson, username, and password.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The PII collected and maintained is the minimum amount required by BRSP for notification and communication purposes, including informing schools of nominations, formally inviting schools to apply for the award, and notifying schools of their recognition as National Blue Ribbon Schools. In addition, throughout the application there are open fields for response based on specific questions. These questions are phrased in a way for responses to be general or discussed in aggregate and are not requesting information about specific individuals.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The sources of the information are from State education agencies, DoDEA, BIE, CAPE, and the nominated schools. State education agencies, DoDEA, BIE, and CAPE nominate the schools for consideration for the awards. The nominated schools complete the applications.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The nominating entities submit school nominations via an online form. The applicants complete an application via an online form.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Once a BRSP nomination is received from a nominating entity, the Department reviews nomination information and notifies principals and superintendents about their nomination and provides an invitation to apply for recognition. It is the responsibility of nominating entities and nominated schools to verify the accuracy of information submitted.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The PII collected and maintained by BRSP is used for notification and communication purposes, including informing schools of nominations and formally inviting schools to apply for the award and notifying these of their recognition as National Blue Ribbon Schools. PII such as username and password is also used to facilitate logging into the BRSP websites to submit nominations and applications.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A link to the privacy policy identified in Question 4.2 is included on the application and also emailed to principals in the invitation letter to schools. Additional notice is provided through the publication of the PIA.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

The BRSP privacy policy can be found at:
https://nationalblueribbonschools.ed.gov/contact/privacy-policy

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Nominating entities have no obligation to nominate schools for BRSP, and school officials have no obligation to complete applications for BRSP recognition once nominated. However, to acquire BRSP recognition, applications must be completed and PII must be provided.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

School information, including the principal's and Superintendent's contact information are shared with the Department's Office of the Secretary, Office of Legislative and Congressional Affairs, and the Office for Civil Rights.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

The information is shared with the Office for Civil Rights to ensure the schools and/or districts have no lawsuits or violations of civil rights statutes and shared with the Office of the Secretary and Office of Legislative and Congressional Affairs for notification to the Secretary of Education, Congress, media, and the public of recognized schools.

External

5.4. Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

Information from recognized schools, such the school name, school address, principal name, school email address, school phone number, and district name are shared with the U.S. Department of Justice (DOJ), Members of Congress, the media, and the general public.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

Prior to recognition of a school, the Department is required to check the list of schools with the DOJ to ensure the schools and/or districts have no lawsuits or violations of civil rights statutes. That list includes school name, address, and district name.

The Department is also required to share the list of schools with Congress (House and Senate). The Department identifies the corresponding congressional districts and notify the members. The information sent to the House is identified by congressional district and includes school name, address, district name, principal name, school email, school phone. The Senate gets the same school information but for all schools recognized from their State.

The notification to the media and public occurs in a press release from the Secretary of Education. The press release includes a link to the National Blue Ribbon Schools website.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☐ N/A

The information about recognized schools is shared by email. In addition, recognized schools for each cohort are published on the BRSP website for recognition purposes and announced in a press release.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

No

5.11. Does the project place limitation on re-disclosure?

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

After the school has received notification of nomination, the principal of that school or another school representative can register for an account to apply for the program. The account creation requires the creation of a username and password to allow them to access their personalized portal within the BRSP site to make any changes and/or edits to the information provided about the school.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

School principals can access a portal within the BRSP website to make any changes or edits to correct inaccurate or erroneous information.

6.3. How does the project notify individuals about the procedures for correcting their information?

Principals are notified by email to log into the portal to verify that all information about their schools is correct. This is done after schools receive their invitation to apply for the award.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Low

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

BRSP is maintained on secure computer servers located in one or more secure contractor network server facilities. Access to BRSP is limited to authorized contractors and Department employees. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, BRSP must receive a signed Authorization to Operate (ATO) from a designated Department authorizing official.

All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. In addition to the enforcement of the two-factor authentication and complex password policy, users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple

access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

Contractors adhere to rules of behavior and Federal laws on the protection of privacy and securing the BRSP system.

All staff assigned to the contract undertake annual required privacy training provided by the Department.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The contractor conducts regular monitoring and auditing of the system including scans and audit logging that sends emails using an event-driven notification system and digests any detection and protection anomalies. In addition, the Department's Office of the Chief Information Officer conducts quarterly scans of the contractor network for vulnerabilities. Firewalls, intrusion detection systems, and intrusion prevention systems are in place and continually monitored.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with BRSP include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.