Privacy Impact Assessment (PIA)
for the

National Blue Ribbon Schools Program (BRSP)
April 25, 2024

Point of Contact

Contact Person: Marcello Rojtman
Title: Information System Security Officer
Email: Marcello.Rojtman@ed.gov

System Owner

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

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

Please complete this ***Privacy Impact Assessment (PIA)****, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The National Blue Ribbon Schools (NBRS) Program is a U.S. Department of Education (Department) program that recognizes outstanding public and non-public elementary, middle, and high schools based on their overall high academic achievement or success in closing the achievement gap among diverse groups of students. The primary goals of the program are spotlighting the best schools in the United States and sharing best practices for outstanding schools.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

The Blue Ribbon Schools Program (BRSP) is a secure data collection and management system consisting of multiple websites and a backend database. 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 Department 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 can 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 to complete the nomination or application process. A representative from the entity may register for an account on the relevant website. Nominated schools also provide information about their specific schools. Representatives of nominated schools, States, and nominating entities are the only members of the public that may access BRSP.

In addition, information may also be collected when individuals use the "Contact Us" page on the BRSP to request assistance or submit questions.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☐ Application
☐ Database	☐ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

Information is collected from nominating entities and nominated schools to facilitate the nominations of and applications by schools for BRSP recognition. Individual information is collected from nominator and school representatives to create accounts in the system. Information such as name, email address, and signature are collected from school principals, superintendents, and school board chairpersons as part of the BRSP application process. In addition, information may be collected through the "Contact Us" page to facilitate responses to questions from members of the general public, typically school personnel.

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

Contractor

[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

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

□ N/A

The contractor's role is to develop and implement system changes, oversee operations, and provide system maintenance as needed.

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

Yes

□ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The National Blue Ribbon Schools Program is authorized by the Department of Education Organization Act, 20 U.S.C. 3402.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☐ Yes

☒ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.
documents include privacy requirements?

N/A

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

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.

The approved schedule for the BRSP is N1-441-09-06, item b. All but one part of BRSP is considered PERMANENT records – see below:

b. Blue Ribbon Schools Program Records the Blue Ribbon Schools Program honors public and private elementary, middle, and high schools that have attained higher levels of performance or that have made dramatic gains in student achievement to high levels, especially among disadvantaged students. Contingent upon funding, final documentation may include guidance document to states, list of schools who received awards for the given year, awards ceremony program booklet and agenda, digital videos and photographs from the ceremony, and representative copies of award certificates.
1. Award records Guidance documents to states, list of schools that receive an award, awards ceremony agendas, and representative copies of award certificates. PERMANENT Cut off annually upon close of program awards cycle. Transfer to NARA after cutoff.
2. DVDs documenting Blue Ribbon Schools Program awards ceremonies. PERMANENT Cut off annually upon close of program awards cycle. Transfer to NARA after cutoff.
3. Digital photographs documenting Blue Ribbon Schools Program awards ceremonies. PERMANENT Cut off annually upon close of program awards cycle. Transfer to NARA after cutoff.

4. Blue Ribbon Schools Program Publications: Publications may include, but are not limited to the awards ceremony program booklet, which contains a Presidential message. PERMANENT Cut off annually upon close of program awards cycle. Transfer to NARA after cutoff.
5. National Blue Ribbon Schools Program master data files: The Office of Communication and Outreach Blue Ribbon Schools Program system is used to document exemplary schools based on the Program criteria. The system data includes electronic applications, information about the exemplary schools, including demographics and the states and schools' assessment results. TEMPORARY Cut off annually upon close of program awards cycle. Destroy/delete 4 years after cutoff.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☐ Home Address
☐ Personal Phone Number	☒ Work Phone Number	☐ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number

☒ Work Fax Number	☒ Digital Signature ☒ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☐ IP Address

☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII:

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:
Name, email address, username, and password.

☒ Federal Contractors

Specify types of information collected from Federal contractors:
Name, email address, username, and password.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State, and local government employees), and the types of information collected from each:[2]

From nominator and school representatives that create accounts to submit materials on the system: username, password, title, name, email address, phone number, and school address.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

From school principals: name, work address, work phone number, work fax number, work email address, signature.

From school district superintendents: name, work email address, work phone number, signature.

From individuals contacting BRSP through the “Contact Us” page: name, school name, address, and email address.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

Information is collected directly from nominator and school representatives that create accounts and complete applications.

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

Information is collected using webforms on the websites listed in Question 1.2.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

The information collected is required as part of the application process to document and recognize exemplary schools. Name, email address, phone number, username, and password are collected from nominator and school representatives to create unique user accounts and to facilitate communication from the Department when necessary. Information including name, email address, and phone number are collected from school principals, superintendents, and school board chairpersons as contact information. School addresses are collected to ensure the accuracy of data submitted as many schools in various locations may share the same name. All information requested as part of applications is available and accessible to the public via internet searches or other State and Federal agency databases.

Information including name and email address is collected from individuals using the “Contact Us” page to facilitate responses to those individuals. School name is required from individuals using the “Contact Us” page as most of these individuals represent schools. Provision of school name is necessary for Department personnel to effectively respond to queries regarding a particular school. School address is collected to ensure the correct school is being addressed, as multiple schools may have the same name.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Nominating entities and nominated schools are responsible for verifying the accuracy of information submitted.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

No

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☑ N/A

3.9.2. If the above answer to question 3.10 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☑ N/A

If the above answer to question 3.10 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☑ N/A

3.9.4. If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☑ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A privacy policy statement is provided on the portal where nominators and school representatives complete applications. Additional notice is provided through the publication of the PIA.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

N/A

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

□ N/A

Privacy Policy: https://nationalblueribbonschools.ed.gov/contact/privacy-policy

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Applying for BRSP is entirely voluntary; however, schools are not eligible for recognition through the program without submission of required materials through the system. Nomination of schools for BRSP by States or other nominating entities is also entirely voluntary.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

□ N/A

Principals' and superintendents' contact information is shared with the Office of the Secretary (OS), Office of Legislative and Congressional Affairs (OLCA), and Office for Civil Rights (OCR).

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

□ N/A

The information is shared with OCR to ensure the schools and/or districts have no lawsuits or violations of civil rights statutes and shared with OS and OLCA for notification to the Secretary of Education, Congress, media, and the public of recognized schools.

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

□ N/A

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

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

□ N/A

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

The Department also shares the list of winning schools with Congress. The Department identifies the corresponding congressional districts and notifies the members. The information sent to the House is identified by congressional district and includes school name, address, district name, principal name, principal email address, and principal phone number. The Senate receives the same school information but for all schools recognized from their State.

The Secretary of Education shares a press release including a link to the BRSP website to the media and the public to publicly recognize winning schools.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

□ N/A

BRSP is authorized by the Department of Education Organization Act, 20 U.S.C. 3402.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

□ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

□ N/A

Information about recognized schools is shared by email, published on the BRSP website, and announced in a press release.

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

□ N/A

No

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

□ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

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 individuals to correct or amend inaccurate or erroneous 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. Nominators and school representatives may also log into the system to correct or amend incorrect information.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

The notification and all procedures to accessing and/or correcting information are included in the invitation letter informing schools of their nomination and inviting the principal to apply for the award on behalf of the school.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☒Low
☐Moderate
☐High

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.

8. Auditing and Accountability

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

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the FPS system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO and with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

BRSP participates in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provide quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. FPS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities. The system owner, in coordination with the ISSO and the Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system.

8.3. What are the specific privacy risks associated with this program or IT 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.