Privacy Impact Assessment (PIA)
for the

Call for Student Performing Artists
(Student Performing Arts Initiative)
May 25, 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: Juliette Rizzo/Project Manager
Contact Email: juliette.rizzo@ed.gov

System Owner

Name/Title: Adrain Walls/Information System Owner
Principal Office: Office of Communications and Outreach (OCO)

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 purpose of the Student Performing Arts Initiative (SPAI) is to afford the U.S. Department of Education (Department), Office of Communications and Outreach (OCO) an opportunity to showcase diverse student performers to enhance the Department's events, specifically those that highlight the Secretary of Education's priorities and initiatives. The student performances will be used to further the Department's mission by enhancing the audio/visual experience of internal and external Department-hosted events, marketed through existing stakeholder channels (e.g., State Education Agency Directors of Arts Education (SEADAE), Assistance for Arts Education listserv through the Office of Elementary and Secondary Education).

   A call for student performing artists will be distributed across the United States and its territories to develop a repository/database of potential student performing artists interested in providing their talents for Department-hosted events. Opportunities have included swearing-in ceremonies, Secretary and Deputy Secretary initiatives, dignitary arrivals, heritage months (e.g., Women's History Month, Hispanic Heritage Month, Asian American and Native Hawaiian/Pacific Islander Heritage Month), and other notable events with celebrities and Cabinet officials. Typically, the Department is interested in including student performances on average 12 times a year.

   Any student performing artist (currently enrolled in an institution of elementary, secondary, or post-secondary education or an accredited trade school), the artist's parent or legal guardian, or any school official[1] will submit a questionnaire form through the Department Online Registration Tool (ORT), formerly referred to as Cvent, a third-party service, backend database, and website accessed through a link from a Department website. All students must be actively enrolled in academic courses at the time of submission.

---

[1] A "school official" is an individual (e.g., teacher, band director, principal, faculty member, professor, vice-principal, art director, or dance instructor) who provides oversight or instruction to students currently enrolled in institutions of elementary, secondary, or post-secondary education or accredited trade schools.

This form will include the student's (18 years old and over), parent/guardian's (if under 18 years old) or school official's name, email address, title (if applicable), phone number, school name, school address, school website, type of school (e.g., public, private, homeschool), type of submission (e.g., adult performer, minor performer, group performance), type of talent, grade level (e.g., elementary, middle), fee, as well as contact information for a primary and (optionally) alternate point of contact (e.g., teacher, principal, other school official) including name, email address, phone number, and title. If a student is under the age of 18, they will also need to provide the information of a parent, guardian, or chaperone, including name, email address, and phone number. In addition, the database will also serve as a vehicle to store required documentation for student performers who are matched to perform (i.e., copyright release waivers, parental consent).

Once a talent match has been identified, the copyright release waiver and parental consent form (for students under the age of 18) will need to be signed and submitted in order for the process to be completed. The copyright release waiver includes name (if the student is under 18, name of the parent/guardian), address, and phone number. If a student is under the age of 18, they will also need to provide a signed parental consent form from a parent or guardian, including name, address, and phone number.

Approved OCO staff will be able to log into ORT using individual usernames and passwords to view submitted applications, which can be sorted by types of talents (e.g., singing, dancing, playing an instrument), grade levels (e.g., elementary, middle, high school), and school types (e.g., public, private, homeschool). OCO staff will be able to use this information to match candidates with available performance opportunities. Information will be stored and accessed within ORT and downloaded into an Excel format and shared amongst approved project managers (Department officials sponsoring an event) in order to review applicable student talent for specific talent requests.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected, used, maintained or shared.

The Department is collecting PII from student performing artists for the purpose of promoting the artists and to enhance the quality of the Departments internal and external events. Students (18+), parents/legal guardians (for students under 18), and/or school officials (for groups of students), will fill out the questionnaire form that will allow the Department to collect PII in order to match student talent, availability to perform at

---

[2] 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

Department events, and to contact the student or point of contact in response to a talent match for specific Department events.

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

New System

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

New PIA

A new PIA for SPAI is being documented, as this is a new Department initiative.

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

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 Department also has authority to perform "public information functions, including the provision, through the use of the latest technologies, of useful information about education and related opportunities to students, parents, and communities." 20 U.S.C. Section 3412(e) (2).

    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)).[3] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

Click here to enter text.

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

Information from ORT is only retrieved by a specific talent (e.g., singer, band, magician), not by a unique identifier.

Records Management
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.

Records are covered under ED 118 (N1-441-08-001). These records are destroyed 2 years after cutoff or when no longer needed for reference, whichever is sooner.

The schedule can be located here: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-education/rg-0441/n1-441-08-001_sf115.pdf

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

---

[3] 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

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.

    Students: name, email address, title (if applicable), phone number, school name, school address, school website, type of school (e.g., public, private, homeschool), type of submission (e.g., adult performer, minor performer, group performance), type of talent, grade level (e.g., elementary, middle), performance fee.

    Primary/Alternate point of contact: name, title, phone number, email address.

    School official, chaperone, or school points of contact: name, address, email address, phone number, title, organization.

    Parents/guardians: name, address, email address, phone number.

    Federal employees accessing the system: 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 SPAI collects only the minimum information necessary. Contact information, such as the individual's name, email address, and phone number, is used to communicate with students/parents/guardians who are interested in performing at Department events. A students age is collected to determine the level of consent needed prior to engaging with the student/parent/guardian.

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

    SPAI collects information directly from students (18+ years of age), parents/guardians (if under the age of 18) or schools (for groups), identifying the student(s) and school point(s) of contact.

    Information is also collected from Federal employees for system administration purposes.

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 Department uses a questionnaire form through ORT that allows for the collection of PII from students that are interested in performing at Department events. In addition to the submission of the application, individuals will also have to submit a photo/video release waivers and parental consent forms (if under the age of 18) in order to be considered for a performance at a Department event.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The SPAI collects information directly from the student (18+ years of age), parent/guardian (if under the age of 18) or school (for groups). It is expected that information submitted to the Department is valid and accurate, as it was submitted by the individual.

Use

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

The Department is looking for official ways to advertise and have students or schools sign up, and this initiative allows the Department to collect personal information, match talent, and contact the students and/or schools for specific Department events.

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

No

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

---

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

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.

The questionnaire form contains a privacy notice. The text of the privacy notice is located in section 4.2. In addition, public notice is provided through this 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

Collection of this information is voluntary. This initiative allows students and/or schools to submit information for an opportunity to perform based on a talent match for specific Department events.

Information Collected: Student name, type of school (e.g., public, private, homeschool), email address, phone number, age range, type of talent, grade level (e.g., elementary, middle), grade (e.g., 8th, 9th), school address, school name. Primary/Alternate point of contact name, tile, phone number, email address. School

points of contact name, address, email address, phone number, title, organization. Parents/guardians name, address, email address, phone number.

Purpose: This form allows the Department to collect personal information about students and/or schools in order to access student talent, availability and to contact the student or point of contact in response to a talent match for specific Department events.

Disclosures: The information will not be disclosed outside of the Department of Education.

Consequences of Failure to Provide information: Collection of this information is voluntary. This initiative allows students and/or schools to submit information for an opportunity to perform based on a talent match for specific Department events. Failure to provide information may leave the submission incomplete and students and/or schools will not be considered for participation at a Department event.

Additional information about this system can be found in the Privacy Impact Assessment.

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?

Students and/or schools submit information to SPAI voluntarily and may decline to provide a submission. However, this may result in a student or school from being considered for participation at a Department event.

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

Information (as identified in Section 3.1) will be stored and accessed within ORT and downloaded into an Excel format and shared amongst approved project managers across the Department (Department officials sponsoring an event) in order to review applicable student talent for specific talent requests.

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

☐ N/A

Information may be shared as required for the purpose of matching talent to events within the Department, for briefing purposes with senior leadership, as well as, for thank you letters and recognition.

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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

---

[5] 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

Click here to select.

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

☑ N/A

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

Click here to select.

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

☑ N/A

Click here to select.

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

   If an individual wishes to access the content of a record in this system, he or she should contact the system owner, identified above in this PIA, with necessary particulars such as name, school, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name.

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

   If an individual wishes to contest the content of a record in this system, he or she should contact the system owner, identified above in this PIA, with necessary particulars such as name, school, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The individual must also provide a reasonable description of the record, specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

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

Procedures for notifying individuals for correcting their information are contained within this PIA.

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

The SPAI falls under ORT. ORT requires an ATO and is currently undergoing an assessment, scheduled for completion by May 2022.

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?

ORT is maintained on secure computer servers located in one or more secure contractor network server facilities. Access to ORT 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, ORT must receive a signed Authorization to Operate (ATO) from a designated Department authorizing official. Security and privacy controls implemented by ORT are comprised of a combination of administrative, physical, and technical controls.

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.

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 following tasks are performed to safeguard ORT information:

- Monthly vulnerability scans performed.
- Annual contingency plan test performed.
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security AuthorizationTeam.
- Annual updates to system security documents.
- Annual mandatory Cybersecurity and Privacy Training for employees and contractors.
- Monthly Continuous Monitoring is in place with vulnerability scans (RA-05), hardware/software inventories (CM-08), and configuration management database updates (CM-06) are posted to CSAM.

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 Office 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.

ORT access is limited/restricted to the Conference and Event Management Services authorized users. The project team member with access to ORT has completed related PII security and privacy awareness training. Standard operating procedures for the purposes of the Call for Student Performing Artists will be created and managed by project leads. It is understood that all PII contained within ORT is for collection/maintenance purposes only and not to be distributed or printed.

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 ORT 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.