Privacy Impact Assessment (PIA)

for the

National Charter Schools Resource Center (NCSRC)

April 24, 2024

Point of Contact

Contact Person: Brandon Dent
Title: Information System Owner
Email: Brandon.Dent@ed.gov

System Owner

Name: Brandon Dent
Title: Information System Owner
Principal Office: Office of Elementary and Secondary Education (OESE)

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 Office of the Charter School Programs (CSP) administers discretionary grants that support the creation of new charter schools[1] and the replication and expansion of high-quality charter schools serving students in pre-kindergarten through grade 12. Funds also support grants to improve charter schools' access to facilities and information dissemination and evaluation activities.

The U.S. Department of Education (Department) is required by Title IV, Part C, Section 4305(a)(3) of the Elementary and Secondary Education Act (ESEA) to reserve funds for the following purposes:

1) Provide technical assistance (TA) to both State entities in awarding CSP subgrants and to eligible entities (the criteria of which are described in the statute) and States receiving CSP discretionary grants;
2) Disseminate best practices regarding charter schools; and
3) Evaluate the impact of the CSP, including the impact on student achievement.

The CSP also funds the National Charter School Resource Center (NCSRC). The NCSRC provides technical assistance to CSP-funded grantees through resources such as case studies, webinars, toolkits, and reports to support the broader charter school sector. The program website can be found at: https://oese.ed.gov/offices/office-of-discretionary-grants-support-services/charter-school-programs/

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

[1] A charter school is a publicly accountable, autonomous school that may operate outside of a traditional public district and functions as a school of choice.

The NCSRC is a website (https://charterschoolcenter.ed.gov/) established using CSP funds that serves as a central location for charter school resources and publications, upcoming events, relevant news, and funding opportunities. The NCSRC website offers a diverse selection of resources on many aspects of the charter school sector for charter school stakeholders and the public. The website enables any user to register for a periodic newsletter on charter school-related topics. The website also enables verified representatives of grantees to register for the community of practice, which is a third-party website that allows verified grantees to exchange grant-related questions and information about the implementation of their grants with each other. Program staff verify the registrants by matching information that exists in the Grant Award Notification maintained in G5. The NCSRC website also includes a "Contact Us" form for general 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)[2] 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.

PII is collected from individuals to create accounts to access the system and to register for the community of practice and/or newsletter. PII may also be collected from individuals requesting information through the "Contact Us" form.

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

Contractor

[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

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

The contractor's role is to develop and implement system changes, oversee operations, provide system maintenance as needed, and apply all applicable security controls to maintain an Authorization to Operate (ATO).

☐ N/A

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 NCSRC is authorized by Title IV, Part C, Section 4305(a)(3) of the Elementary and Secondary Education Act of 1965 (ESEA), as amended by the Every Student Succeeds Act, P.L. 114-95.

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.

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):

The applicable ED records schedule is 254: Grants Administration and Management Files (N1-441-11-001). Records are destroyed 10 years after the last action is taken on the file, but longer retention is authorized if required for business use.

☐ 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:

While no PII is solicited through the website's discussion board or "Contact Us" webpage, any information contained in any community of practice posts or sent to the Department through the "Contact Us" webpage will be maintained in the system.

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, and password.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Name, email address, 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:[3]

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

Individuals registering for the newsletter: name and email address.

CSP grantee representatives registering for the community of practice: name, email address, password, organization, and optional photo. While no PII is solicited through the website's discussion boards, any information contained in the community of practice posts will be maintained in the system.

Any individual submitting a request for information or assistance through the "Contact Us" form: name 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 individuals using the "Contact Us" form or registering for newsletters or the community of practice.

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

For the "Contact Us" webform, information is obtained through the NCSRC website. For the newsletter and community of practice, individuals use a link on the NCSRC website to access a third-party webpage to provide their information. Newsletter registration is hosted through Constant Contact while the community of practice is hosted through Groupsite.

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.

Name, email address, and password are collected from Federal employee and contractor system administrators and community of practice registrants as the minimum information required to create unique access credentials. Organization is collected from community of practice registrants to verify that they are associated with a CSP grantee. Photographs are optionally collected from community of practice registrants if they wish for an image to appear in their profile. Name and email address are collected for the newsletter and the "Contact Us" form as contact information for sending the newsletter or requesting a response.

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)?

Constant Contact sends an email to individuals who register for the newsletter to confirm their request. Email addresses that return "undeliverable" messages are purged from the system.

When an individual registers for the community of practice, Groupsite sends an email to CSP program staff, who match the registrant's information with information maintained in G5. Once CSP program staff confirm the registrant's identity, Groupsite sends a confirmation email to the user. NCSRC contractor staff audit Groupsite accounts weekly, disabling accounts of individuals no longer associated with a CSP grantee.

Individuals submitting requests through the "Contact Us" form are responsible for ensuring the accuracy of their information.

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

3.9.4. 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

3.9.5. 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.

The NCSRC website maintains a privacy policy. Public notice regarding NCSRC's collection and use of PII is also provided by this 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?

Yes

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

https://charterschoolcenter.ed.gov/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.

Requesting information or assistance through the "Contact Us" form is entirely voluntary and is only used to respond to the request submitted through the form. Registration for the newsletter and community of practice is entirely voluntary and newsletter subscribers and community of practice members can opt out at any time.

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.

No

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

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

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.

No

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

☑ N/A

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

☑ N/A

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

☑ N/A

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

☑ N/A

Click here to select.

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

Click here to select.

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

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

Click here to select.

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

Click here to select.

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.

"Contact Us" information is not maintained on the system after the request has been completed. Newsletter subscribers can unsubscribe at will. Community of practice members can access, change, and delete their information through the NCSRC website.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

"Contact Us" information is not maintained on the system after the request has been completed. Newsletter subscribers can unsubscribe at will. Community of practice members can access, change, and delete their information through the NCSRC website.

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

Newsletter subscribers are notified of the ability to opt-out through an "unsubscribe" link found at the bottom of every newsletter email. Community of practice members can access the "My Account" section of the website to access and modify information.

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?

Access to the system is limited to authorized NCSRC program personnel and contractors responsible for administering the NCSRC program. Information collected on the NCSRC website is accessible only to authorized users. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), NCSRC must receive a signed ATO from a designated FSA official. FISMA controls implemented by NCSRC are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and accept a Rules of Behavior, and are required to utilize a complex password and two-factor authentication.

Physical safeguards include storing data in a secured data center, access to which is controlled by multiple access controls. All sensitive data are encrypted in transit and at rest and access to records is strictly limited to those staff members trained in accordance with the Privacy Act of 1974, as amended.

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 NCSRC 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. Through this process, a variety of controls are assessed by an independent assessor to ensure the NCSRC system and the data residing within are appropriately secured and protected.

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.

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

NCSRC participates in the Department's Ongoing Security Authorization (OSA) program. As part of the OSA program, quarterly assessments are conducted by an independent Security Assessment Team (SAT) on a continuous basis throughout each fiscal year. Any findings from the quarterly assessments are tracked via plans of action and milestones (POA&Ms). System stakeholders, including the ISO, ISSO, and contractor support team (CST), are responsible for monitoring the status of privacy and security control implementation and ensuring controls are updated accordingly. Implementation statements, security documentation, privacy documentation, vulnerability scanning, and testing results are stored, tracked, and updated in the Cybersecurity Assessment and Management (CSAM) system. Furthermore, the ISO also continuously monitors and tracks the overall cybersecurity posture of NCSRC through the Department's Cybersecurity Framework (CSF) Risk Scorecard. The scorecard provides a snapshot of the system, including information such as an overall score, system discrepancies, POA&Ms, and security documentation.

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 NCSRC 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 or embarrassment. Organizational harm may include a loss of public trust, legal liability, and remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and limiting users to those who are screened, utilizing least privilege principles and encrypting data in transmission. To further mitigate risk, the following safeguards have been implemented:

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

Risks are also mitigated by updating security patches and updating devices' operating software. 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.