Privacy Impact Assessment (PIA)

for the

Analytic and Data Support to States for 21st Century Community Learning Centers

June 7, 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: Daryn Hedlund/Management and Program Analyst
Contact Email: Daryn.Hedlund@ed.gov

System Owner

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

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.

Analytic and Data Support to States for 21st Century Community Learning Centers (21st CCLC), is a cloud-based technology solution for the collection of information on the 21st CCLC formula grant program. The 21st CCLC program is a State formula grant program authorized under Title IV, Part B, of the Elementary and Secondary Education Act (ESEA), as amended by The Every Student Succeeds Act (ESSA) of 2015, in which each State receives a grant based on its share of ESEA Title I, Part A funds. States must use their allocations to make competitive awards to eligible entities. 21st CCLC uses a browser-based web application called 21APR to collect annual reports from schools and other organizations receiving Federal funding through the 21st CCLC program (grantees) and State education agencies (SEAs) pertaining to Government Performances and Results Act (GPRA) performance. The system collects de-identified, aggregated data at the program level on activities, staffing types, participation, and GRPA outcomes. These data are entered by school and SEA representatives through a portal within the 21APR application.

Authorization for access to 21APR consists of three tiers. U.S. Department of Education (Department) staff and contractor "super users" are able to grant access to SEA representatives. These SEA representatives are then given the ability to grant access to school and other organization points of contact so program-level data can be submitted to the portal. Information collected from all users includes name, email address, and password, with associated State also being collected from applicable users.

The 21st CCLC system is hosted within the Amazon Web Services (AWS) cloud service provider (CSP) environment. The 21st CCLC solution stack consists of Linux, Apache HTTP Server, MySQL database, and PHP (LAMP).

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

[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

used, maintained or shared.

Name, email address, and password are collected from all users for account creation. Associated State is collected from grantee and SEA points of contact.

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?

New PIA

During a review of 21st CCLC, it was determined that a PIA is required for this system.

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 21st CCLC program is a State formula grant program authorized under Title IV, Part B: 21st Century Community Learning Centers, of the ESEA, as amended by ESSA of 2015, in which each State receives a grant based on its share of ESEA Title I, Part A funds. States must use their allocations to make competitive awards to eligible entities.

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 name or other personal identifier. Information is retrieved by entity or institution name (e.g., school, community-based organization like a YMCA).

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.

The applicable Department records schedule is ED 254: Grants Administration and Management Files (N1-441-11-001). Records are destroyed 5 years after last action is taken on the file, but longer retention is authorized if required for business use.

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

[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

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, email address, and password are collected from all users for account creation. Associated State is collected from grantee and SEA points of contact.

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 21st CCLC to establish user accounts for the purpose of collecting annual reports from schools and other organizations receiving Federal funding through the 21st CCLC program (grantees) and SEAs pertaining to GPRA performance.

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

Department users and SEA representatives.

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

Information from Department users is collected from the individual and then manually entered into a web form by an authorized user during the account registration process. Information from grantee and SEA points of contact is manually entered through a portal within the 21APR application by an authorized user. The webform is only accessible by authorized users and registration is done on behalf of the user by an authorized user.

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?

PII is validated through the use of restricted form filling and account verification through an account activation email. Information is validated by the authorized user prior to creating an account on behalf of other users that require access.

[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.

Use

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

Name, email address, and password are used to create and maintain user accounts. Name and work email address are used for contact purposes for each program.

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

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.

SEAs, school and other organization points of contact provide their information in order to gain access to the 21st CCLC portal. The PII collected and maintained to establish user accounts for the purpose of collecting annual reports from schools and other organizations receiving Federal funding through the 21st CCLC program (grantees) and SEAs pertaining to GPRA performance. Notice of how their information is handled once submitted to the Department is provided through the publication of 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

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?

Individuals can choose to not provide information to create an account but doing so will prevent access to the system.

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?

☑ N/A

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.

No

5.2. What PII will be shared and with whom?

☑ N/A

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

☑ N/A

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.[4]
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.

5.8. 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

[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.

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 requires access to their information maintained in 21st CCLC, they may obtain access by logging into their online account through 21APR.

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

Authorized users can edit their name, email address, and password in their profile within the system.

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

Authorized users have access to their information in their profile within the system. Each field for name, email address, and password are editable within the user's profile page in the system. In addition, this PIA notifies individuals about the procedures for correcting their 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 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?

Access to the system is limited to authorized 21st CCLC program personnel and contractors responsible for administering the 21st CCLC program. Authorized personnel include Department employees and contractors. The system limits data access to Department and contract staff on a "need to know" basis and controls individual users' ability to access and alter records within the system.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), 21st CCLC must receive a signed ATO from a designated authorizing official. FISMA controls implemented by 21st CCLC 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.

The server is located in a secure room, with limited access only by those who are authorized to access. Further, all physical access to the site where the server is maintained is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

In addition, 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.

Weekly scans are performed in support of code migrations and/or system fixes. Quarterly authenticated network and operating vulnerability scans, along with network penetration testing, are conducted to ensure the security of the 21st CCLC environment. As part of an ongoing security and authorization process, security audits are performed on an annual basis by authorized independent third parties to ensure the controls in place are effectively securing our data. 21st CCLC is required to submit Plans of Actions and Milestones (POA&MS) quarterly which continuously monitor any vulnerabilities and ensure that they are mitigated and closed. Additionally, self-assessments are conducted annually.

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 ensures that the information is used in accordance with stated practices in this PIA through several methods. One method is completing the Department Risk Management Framework process and receiving an ATO. Under this process a variety of controls are assessed by an independent assessor to ensure this system and the data residing within are appropriately secured and protected. One-third of all controls are tested each year and the entire system security is reevaluated every three years. The PIA is reviewed and updated on an as needed basis and, at a minimum, every two years.

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 21st CCLC 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 credential theft, and/or embarrassment. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, encrypting PII stored in the database, 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 these risks, 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 device operating software, amongst other software updates. 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.