Privacy Impact Assessment (PIA)

for the

Comprehensive Literacy State Development (CLSD) Grants

December 4, 2023

Point of Contact

Contact Person: Anuritha Bezwada

Title: Information System Owner

Email: anu.bezwada@ed.gov

System Owner

Name: Anuritha Bezwada

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 Comprehensive Literacy State Development (CLSD) program is a discretionary grant program for State education agencies (SEAs) authorized under the Elementary and Secondary Education Act (ESEA). CLSD grants are intended to create a comprehensive literacy program to advance literacy skills, including pre-literacy skills, reading, and writing, for children in preschool to grade 12, with an emphasis on disadvantaged children, including children living in poverty, English learners, and children with disabilities.

The Striving Readers Comprehensive Literacy (SRCL) program is also authorized pursuant to the ESEA. SRCL administers discretionary grants and set-aside grants for the Secretary of the Interior for schools funded by the Bureau of Indian Education and four Outlying Areas – American Samoa, Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands.

The SRCL grant program is ending and will transition into being included within the CLSD grant program by the summer of 2023.

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

The CLSD system is a web application used as a tool to monitor the progress of the grants once they have been awarded. The grant application process takes place in the U.S. Department of Education (Department) G5 system, outside the CLSD system. The system enables grantees to submit the percentage of completion of grant-related tasks, percentage of grant funds spent on various categories, and summaries of project-specific work completed through quarterly and annual reports. Each grantee will only be able to access and modify the reporting for the grants they are awarded. Grantees have the capability to upload supporting documents if needed.

The website offers information and resources about planning, implementing, and evaluating literacy programs, as well as a platform for grantees to collaborate with other SRCL and CLSD grantees. The website contains documents regarding best practices and innovative approaches as well as other resources including evidence-based practices, tools and recommendations for practice, and news about professional learning events.
The CLSD website also includes a discussion forum for SRCL and CLSD grantee representatives to communicate and discuss topics pertaining to literacy programs.

Authentication is required for grantees to submit and review reports as well as to access the discussion forum. Grantees log in to the system using username and password. Grantees submit updates regarding various categories and narratives of activities regarding literacy programs. Federal employees monitoring the program log in to the system to view the submitted updates to review the statuses of the grants.

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.

PII is collected to create user accounts for grantee representatives and system administrators. Grantee representatives use their accounts to submit quarterly performance reports detailing the status of their grants and to participate in the system's discussion forum. System administrators use their accounts to review submitted performance reports and monitor the discussion forum.

[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

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

Contractor

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

□ N/A

The contractor manages the website through system and web content administration. The contractor uploads web content and data that are approved and provided by the Department program office.

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.

CLSD's collection and use of data are authorized by Sections 2221-2225 of the Elementary and Secondary Education Act of 1965, as amended by the Every Student Succeeds Act (20 U.S.C. §§ 6641-45).

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):

General Records Schedule (GRS) 1.2, item 020: Grant and Cooperative Agreement Case Files for Successful Applications:
Retention: TEMPORARY. Destroy 10 years after final action is taken on 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: The website contains a platform for grantees to collaborate, share ideas, experiences, and lessons learned with other SRCL and CLSD grantees. As part of this platform, any type of information can be shared, but participants are urged not to provide any sensitive information regarding themselves or personal matters.

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, work phone number, work email address, username, password.

☒Federal Contractors

Specify types of information collected from Federal contractors: Name, work phone number, work email address, username, 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 grantee representatives: name, work phone number, work email address, work address, username, password.

While no specific information is solicited through the discussion forum, any information included in discussion board posts will be maintained on the system.

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)?

Grantee representatives provide PII required to create accounts in CLSD to the CLSD program office via email. The program office then relays that information to CLSD system administrators, who create accounts in the system. System administrators also create accounts for Department employees and contractors accessing the system.

Quarterly and annual reports are submitted to the system by grantee representatives.

Grantee representatives post information in the discussion forum.

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

PII is received from grantee representatives via email and stored in a backend database. Department program officers notify system administrators via email of Department employees and contractors that require access to the system.

Quarterly and annual reports are submitted through a portal on the website.

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

Information is posted in the discussion forum by grantee representatives.

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, username, and password are necessary to establish accounts in the system and ensure that each account is attached to only one individual. Phone number and work address are collected from grantee representatives as contact information in case the CLSD team needs to contact grantees regarding discrepancies or errors in submitted reports.

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)

The information posted in the discussion forum is only accessible to users who are logged in to the system and is not accessible to the general public. Other than the discussion forum, grantee representatives can access only their own information.

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)?

Federal program officers conduct quarterly monitoring calls with grantee representatives to provide guidance regarding grants and policy updates. During these calls, program officers ask grantee representatives about any staff changes that may have occurred. Grantee representatives also notify Department program officers of personnel changes via email.

The system sends a confirmation email to the email address supplied during the account creation process to verify users' contact information. Users are otherwise responsible for ensuring the data on the website are correct.

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

3.10.2. 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

3.10.3. 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.

There is a privacy policy listed at https://literacycenter.ed.gov/privacypolicy.aspx.

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

Click here to select.

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
Our website contains a discussion board for grantees to collaborate with other Striving Readers Comprehensive Literacy (SRCL) and Comprehensive Literacy State Development (CLSD) grantees. Through this board, you can voluntarily submit personal information, such as your name or e-mail address. Submitted information is used only for the purposes described on the discussion board and is not made available to any third party outside of the system. However, when you submit a comment to the discussion board, if you supply your name, e-mail address, or other personal information, that information is posted along with your comment and is viewable by other members of the discussion board.

This website contains links to other sites. Please be aware that the CLSD is not responsible for the privacy practices of these sites. Also, when users leave our site, we encourage them to read the privacy policies of every website that potentially collects personally identifiable information.

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.

Quarterly and annual reports are required submissions for grantees; the status of a grant would be adversely affected by not submitting reports. Information must be collected from grantee representatives to create accounts on the system that are necessary for submitting the required reports. Information submitted to the discussion forum is 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.

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

Note that any PII provided on the website’s discussion forum will be made available to other participants on the discussion forum.

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.

Grantee representatives can view and verify their information by logging into the CLSD website.

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

Grantee representatives must contact CLSD system administrators via email to make changes to their information. Contact information for CLSD system administrators is available on the website. System administrators reply to grantee representatives requesting changes via email to verify the request before a correction is made.

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

A user guide is available on the CLSD website that provides instructions on correcting information. Webinars for CLSD grantees are also conducted on an as-needed basis outside the system; these webinars provide instructions on correcting information in the CLSD system.

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?

No – System currently under development

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?

Administrative access to the system is limited to authorized Department personnel and contractors responsible for administering the CLSD program. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), CLSD must receive a signed ATO from a designated official. FISMA controls implemented by CLSD 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 rules of behavior, and are required to use a complex password and two-factor authentication. Users receive a one-time passcode via email when attempting to log in as part of the two-factor authentication process.

Accounts with no activity for 365 days are marked as deactivated by system administrators. Accounts can also be deactivated by a modification request or employee termination or transfer. When a system administrator receives a notification that a user has been terminated, transferred, moved, or their job function requires a different access level, the administrator can modify or delete accounts as required. Unless the account has already been removed, deactivated accounts can be reactivated by contacting system administrators and going through the modification process.

CLSD maintains a list of all user accounts with their related access privileges. This list is reviewed annually for compliance with account management requirements. Privileged accounts for system administrators are reviewed and recertified quarterly.

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 first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, CPS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of 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 and meets regularly with the ISSO.

The system owner conducts periodic audits to ensure that PII is used in accordance with this PIA. The system owner ensures that the system security and access control plans are being executed correctly. For example, system administrators maintain a list of all user accounts with their related access privileges. This list is reviewed annually for compliance with account management requirements. Privileged accounts for system administrators are reviewed and recertified quarterly.

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

CLSD is required to obtain and maintain an ATO. This process includes an independent assessment of all required security and privacy controls and produces plans of action and milestones (POA&Ms) to ensure any deficiencies are remediated. CLSD will also participate in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security and privacy controls are in place and working properly.

In addition, CLSD has a system security plan that ensures the application is secure and monitored on a timely basis. As part of normal user access, system administrators identify users that need access to CLSD and initiate the request for access to the system. Accounts that are inactive for more than 90 days are marked as disabled. Disabled accounts can be reactivated by contacting the system administrator. Accounts with no activity for 365 days are marked as deactivated. Accounts can also be deactivated by a modification request or because of employee termination or transfer.

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 CLSD 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 embarrassment or loss of credentials that are used to gain access to other resources. 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 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.