Privacy Impact Assessment (PIA)

for the

National Center on Safe Supportive Learning Environments (NCSSLE) Website System

September 2, 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: Brandon Dent/Information System Owner
Contact Email: Brandon.Dent@ed.gov

System Owner

Name/Title: Brandon Dent/Information System Owner
Principal Office: Office of Elementary and Secondary Education

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 National Center on Safe Supportive Learning Environments (NCSSLE) which is operated by a contractor, the American Institutes for Research (AIR), is funded by the U.S. Department of Education (Department) Office of Safe and Supportive Schools within the Office of Elementary and Secondary Education (OESE) to help address many factors that impact the conditions for learning in schools and communities, such as bullying, harassment, violence, and substance abuse. Specifically, the Center:

- Provides training and support to state administrators, school and district administrators, institutions of higher education, teachers, support staff at schools, communities and families, and students; and
- Seeks to improve schools' conditions for learning through measurement and program implementation, so that all students have the opportunity to realize academic success in safe and supportive environments.

The NCSSLE website serves as a central information repository for the center. It includes information about NCSSLE's training and technical assistance, products and tools, and latest research findings.

AIR also supports a portal for several Department-funded grant programs via NCSSLE, including the Project Prevent, Mental Health Professional Services, School Based Mental Health, and Trauma Recovery grant programs. The portal is a technical assistance initiative designed to support the collaboration of the grantees in administering and implementing their respective grants. Grantees use the portal to:

- Find resources grantees have developed or are using,
- Engage in discussions with peers, and
- Access technical assistance specialist (TAS) contact information that can assist them in administering and implementing grant programs.

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

NCSSLE Website: The NCSSLE website displays names of Federal employees, as well as names and email addresses of NCSSLE leadership in the "About" section of the website to allow users to contact NCSSLE staff for assistance.

Grantee Portal: For grantees, PII is initially collected individually via applications that the State education agency (SEA) / Local education agency (LEA) submitted to the Department after ultimately receiving their grant award. As NCSSLE works with the grantees, staffing changes are shared with the Federal Program Officer(s) (FPO) and posted in the Department's grant management system, the G5 system, as well as shared, often via email, with their respective TAS. Use of the grantee portal, including posting pictures, helps to create a community among participants. Also, while the contact information is not visible to other users, the system sends out individual notifications set at the frequency each user prefers with updates, so users are aware of when and what content is posted in the portal. For example, content posted in the portal include information on upcoming grantee events users may wish to attend and resources discussed during community of practice calls they wish to explore in more depth.

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 NCSSLE, 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

[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

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 legal authorities for NCSSLE are Title IV of the Higher Education Act of 1965 (HEA), Part A, Subpart 1 (Student Support and Academic Enrichment Grants – 20 U.S.C. 7111-7122) and section 4631 (National Activities for School Safety – 20 U.S.C. 7281) of the Elementary and Secondary Education Act of 1965 (ESEA), as amended.

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

Information is not retrieved from the system by a unique identifier. Information is collected to display contact information and to create user accounts. Grantee portal users who need to reset a password can do so within the NCSSLE grantee portal.

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] 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

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.

This system is under review for its revised record retention and subsequent NARA approval. Records will be safeguarded as permanent pending NARA approval.

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

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.

NCSSLE Leadership: The NCSSLE website displays names of Federal employees who oversee NCSSLE (Contracting Officer's Representative (COR) and subject matter lead) and/or the leads for the grant programs (Federal Program Officers, or FPOs) in the "About" section of the website. It also posts the names and email addresses of NCSSLE leadership in the "About" section of the website.

Grantees: The grantee portal collects and maintains the first and last names, username, password, business contact information (email address, city, state, job title, affiliation), and potentially a photo for each individual if they choose to post one.

TASs: The grantee portal also collects and maintains TAS contact information. The information collected are the first and last names, username, password, business contact information (email address, city, state, job title, affiliation), and potentially a photo for each individual if they choose to post one.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

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

NCSSLE Website: The PII for Federal staff is collected from the NCSSLE's main point of contact at the Department or from the COR. The PII for NCSSLE leadership is collected from the director or deputy director based on the contract.

Grantee Portal: For grantees, PII is initially collected individually from PDF applications that the Department sends NCSSLE leadership for SEAs and LEAs that received a grant award via the Department granting process that NCSSLE will support. As NCSSLE works with the grantees, staffing changes are shared with the FPO and posted in the G5 system, as well as shared, often via email, with their respective TAS. The Department conveys these updates to NCSSLE leadership. NCSSLE maintains a private database of grantee contact information and technical assistance interactions within AIR's Technical Assistance Tracker (TA Tracker). Any official changes are updated within both the TA Tracker and grantee portal accordingly.

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

NCSSLE Website: The PII for federal staff, or names of Office of Safe and Supportive Schools (OSSS) leadership, is typically conveyed by the COR or subject matter expert/main point of contact from the Department during biweekly check in calls with NCSSLE's director and deputy director. On occasion, a FPO will also share an update that AIR later confirms with the COR and subject matter expert before updating the PII on the "About" section of the NCSSLE website. The PII for NCSSLE leadership is collected from the contract's list of key personnel and confirmed organizational chart.

Grantee Portal: The Department sends AIR PDFs of applications for SEAs and LEAs that received a grant award via the Department granting process that NCSSLE will support. AIR collects the PII from the PDF applications and enters it into the TA Tracker and portal. PII for staff is collected based on AIR's contract information. To enter the PII into the portal, a set of NCSSLE staff have administrative rights to the portal and enter the PII into the grantee portal one by one, thereby creating a profile for each grantee with an initial password. Grantees are instructed to update their password and other PII when they log into the system for the first time.

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?

[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.

NCSSLE Website: The COR notifies AIR of any staffing changes. When there is a change (e.g., retirement, change in role), AIR updates the "About" section on the NCSSLE website.

Grantee Portal: NCSSLE TASs receive updates from the grantees verbally and/or via chat as they meet with them for check in calls or via email (share new staff, including name and email); AIR confirms the change with the Department and then updates their TA Tracker and the portal (e.g., change in project director or change in contact information). NCSSLE TASs actively work with the grantees (monthly individual check ins, monthly group technical assistance events), thus contact information is confirmed on an ongoing basis. If NCSSLE does not hear back from a grantee, they work with the Department's FPO who is responsible for overseeing the grants to confirm contacts; all contacts must be updated in the Department's G5 system.

Use

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

NCSSLE Website: The contact information on the NCSSLE website is displayed for easy access, correspondence, and assistance purposes. For example, an organization wishing to partner with NCSSLE can find out who the director is and send him / her an email to initiate contact.

Grantee Portal: PII is used to create accounts in the portal. The purpose of using the portal is to create a community among grantees and NCSSLE staff in engaging in the work of the grants. Grantees can talk with each other without seeing contact information. Also, as NCSSLE posts resources and events in the portal, as well as when new discussion threads are started, grantees receive notifications at the frequency they prefer. This allows them to get information that will help support the implementation of their grant.

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.

The NCSSLE system provides notice to individuals through privacy policies located on its websites and through the publication of this PIA.

NCSSLE Website: There is a Privacy Policy linked on the footer of the website: https://safesupportivelearning.ed.gov/privacy-policy.

Grantee Portal: There is a Privacy Policy linked to the "Log In" webpage: Terms of Use / Privacy Policy | NCSSLE Grantee Portal. AIR also informs grantees about the portal. When a grantee is granted access to the system, they are aware of the information included and how it is shared (within password protected system, only staff access the information). They have opportunities to update or change the information in the system, including whether to share with others. The system also allows a user to allow other users to contact them while hiding their email address.

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

NCSSLE Website: To review the text of the Privacy Policy located on the NCSSLE website, visit the link: https://safesupportivelearning.ed.gov/privacy-policy.

Grantee Portal: To review the text of the Privacy Policy located on the NCSSLE grantee portal, visit the link: Terms of Use / Privacy Policy | NCSSLE Grantee Portal (ed.gov).

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?

NCSSLE Website: If a Department or NCSSLE staff person would like to be removed from the "About" section, they can contact AIR any time, and AIR can immediately remove their name or update the webpage as needed. All are aware their name is posted; staff are aware their business email is posted as well.

Grantee Portal: There are a few opportunities for grantees to consent to use, decline, or opt out of using the portal:

1. When NCSSLE TASs discuss the portal with grantees, whether it is a new member coming mid-grant or new members at the start of a new grant program, they describe how it as optional, what information is shared within, and how the NCSSLE staff use it. Each user must have approval of their grantee project director (PD) to join; grants tend to have a PD and other staff supporting the grant work. If someone does not want to become a portal user, they can inform NCSSLE staff and AIR will not create an account.
2. As users engage in the portal, they can reach out to their TAS anytime to be removed from the portal.

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 Department 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

As NCSSLE works with the grantees, staffing changes are shared with the G5 system to ensure accuracy and the integrity of contact information for grantees.

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

☑ N/A

See the response for question 5.2.

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

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

☑ N/A

5.6. Is the sharing with the external entities authorized?

☑ 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.

5.7. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

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

☑ N/A

5.9. 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

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

☑ N/A

6. Redress

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

NCSSLE Website: Department and NCSSLE staff can access the publicly available webpage where their PII is posted.

Grantee Portal: Each user has access to their PII via their account profile within the system. When they log in for the first time, they are instructed to update their business related PII, and can correct or remove information they do not want included within the system. They can change their information within the system at any time. A User Guide provides instructions on how to update a user profile.

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

NCSSLE Website: The individual can email NCSSLE leadership, and AIR will immediately update the webpage.

Grantee Portal: When a user logs in for the first time, they are instructed to update their PII, and can correct or remove information they do not want included within the system. They can change their information within the system at any time. A User Guide provides instructions on how to update a user profile. They also can reach out to their TAS for assistance in updating the portal profile.

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

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?

Administrative Controls:
Administrative controls include an admin access evaluation to limit number of individuals with access to PII, system security plan, contingency plan, data back-ups, least privilege controls, incident response training and exercises, security awareness and role-based training for users and administrators, and retention and destruction as per the data plan. AIR implements separation of duties between users, developers, IT Systems Administrators, and Infosec staff using role-based access control (RBAC) in Active Directory. AIR developers are not permitted to access production applications and databases in Azure-hosted production systems; changes to production systems are executed by administrators. AIR also provisions separate user accounts for standard and privileged accounts.

Technical Controls:
This environment is protected by a firewall, advanced malicious code protection, and the Azure cloud security framework. AIR implements multi-factor authentication for IT system administrators to manage the hosting environment and for developers to manage

the web application and database. AIR employs strong password policy (password length, complexity, uniqueness, lockout) with all passwords stored as a hashed value in Active Directory using government approved secure hashing of the password. Other technical controls include identity and access management, security auditing, US Government-approved encryption of data at rest and during transport, 24x7 event monitoring by trained security operations staff, and penetration testing.

Physical Controls:
Physical controls are fully documented and independently verified as part of Azure's FedRAMP certification. These include a hardened data center that employs an armed guard force, multi-layered biometric access, electronic access auditing, video surveillance, and the use of cages for physical separation.

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.

AIR performs continuous monitoring of system and web application vulnerabilities and threat information to reduce chance of unauthorized access to PII. Vulnerability and threat information is reviewed weekly as part of a formalized weekly process involving IT, development, and information security staff. Threat information and security logs are monitored 24x7 by trained security operations staff.

AIR conducts periodic testing and assessments appliable to this system that include security controls assessments of applicable NIST controls in System Security Plan, weekly vulnerability scans, monthly web application and database vulnerability scans, incident response and contingency plan testing, and annual penetration testing.

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 both PTA and PIA forms and ensure both are accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. Under this process an independent assessor assesses a variety of controls to ensure the system and the data residing within are appropriately secured and protected. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. These methods along with regular communication with NCSSLE users ensure that the information is used within the stated practices outlined in this PIA.

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 the NCSSLE website include the exposure of PII that in this case includes business contact information that could be used to perpetrate targeted phishing emails or embarrass the user. Other privacy exposures can involve the user credentials, that if harvested by a threat actor, can be used to perform unauthorized access, commit fraud or other computer crimes that are potentially hazardous to both individuals and organizations. Examples of 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:

- Encryption of data in transit (e.g., during login session) using US Government standard TLS.
- Continuous Security Monitoring of System Logs, Malware Prevention, Availability and System Health through Azure Sentinel and 24x7 Security

Operations Center

- Weekly security controls monitoring
- Monthly Web Application, Database and Vulnerability Scanning
- Annual contingency plan test
- Annual or ongoing security assessments
- Annual cybersecurity and privacy training for Department users

Risks are also mitigated by updating security patches and updating devices operating software, amongst other 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.