Privacy Impact Assessment (PIA)

for the

Student Support and Academic Enrichment Program (Title IV Part A) (T4PA)

February 8, 2021

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
Contact Email: brandon.dent@ed.gov

System Owner

Name/Title: Hamed Negron-Perez
Principal Office: 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.

The Every Student Succeeds Act (ESSA) and Elementary and Secondary Education Act (ESEA) are dedicated to creating equity of opportunity for all elementary and secondary students, allowing them to access a high-quality education with a new path toward comprehensive student success. These laws provide elementary and secondary students with a well-rounded education, safe and healthy environments, career readiness, and tools and resources for achieving digital competency and learning via the effective use of technology. To administer these laws, the Office of Safe and Supportive Schools (OSSS) within the U.S. Department of Education (Department), through the Student Support and Academic Enrichment Program Title IV Part A (T4PA) Technical Assistance Center, provides high-quality technical assistance, training, and support to State Educational Agencies (SEAs) to increase their capacity to assist Local Educational Agencies (LEAs) in implementing Student Support and Academic Enrichment Program (SSAE) program activities.

Under subpart 1 of Title IV, Part A of the ESEA, known as the SSAE program, each SEA is given the freedom and flexibility to determine the best approach to successfully implement the SSAE program for the students, schools, and LEAs within their jurisdiction. The OSSS provides assistance to SEAs through the T4PA Technical Assistance Center, which utilizes a public-facing website that is regularly updated by the T4PA Center Team. The T4PA system consists solely of this website, which includes three elements: information posted to a portal accessed by SEA and LEA representatives (e.g., resources, event calendars, reports, and best practices), discussion boards for these representatives to communicate with each other, and a portal for the representatives to submit technical assistance requests. The discussion boards are accessible only through use of users' login credentials. The T4PA system is hosted on the Amazon Web Services (AWS) GovCloud. The server is composed of an Internet Information Services webserver and Structured Query Language Server backend.

The SEA and LEA designate representatives to access the website. These SEA and LEA points of contact register on the T4PA website in order to obtain login credentials. The T4PA system collects personally identifiable information (PII) from these points of contact solely for the purpose of producing login credentials for the website.

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

Information collected is used to provide login credentials to access the system, which is a website that is used to disseminate T4PA guidance information and facilitate collaboration among SEAs and LEAs using discussion boards for sharing best practices and success stories.

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

There are no changes to the system, but it was determined by Department officials during a recent review of the system that the system maintains PII. As a result, the PTA needed to be revised, a PIA needed to be drafted, and privacy controls needed to be selected and implemented.

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.

[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

The program is authorized by Title IV, Part A of the Elementary and Secondary Education Act (ESEA), as amended. The program regulations are in the U.S. Code of Federal Regulations at 34 CFR 222. These allow for the establishment and maintenance of the program, including determining LEA eligibility and for auditing eligible LEAs.

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

Click here to enter text.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☐ N/A

A SORN is not required because the information is not retrieved by a name or other identifier.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

GRS 3.2, item 030 – Information Systems Security – Records are destroyed 10 years after last action is taken on the file, but longer retention is authorized if required for business use.

[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

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes. All PII is disposed of upon termination of the system and per the Department's Records Disposition schedule (see: https://www2.ed.gov/notices/records-management/index.html)

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.

- SEA and LEA designated point of contact (POC):
  - First Name
  - Last Name
  - Organization email
  - Organization phone
  - User ID
  - Password

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

Yes

The system collects only name and contact information to establish user accounts for the website. This is the minimum PII necessary to establish the accounts. Organization phone number is collected to provide contact information for resolving technical assistance requests.

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

Information is provided by LEA and SEA POCs

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

SEA and LEA POCs request a user ID and the webmaster creates the user ID using an administrative interface. The password is generated automatically by the system and is emailed to the 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?

The program office directly contacts the LEA and SEA to verify the contact details through a confirmation email. The user is responsible for making updates and ensuring the data on the website are correct.

Use

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

The information collected is used to create user login credentials to allow the users to communicate using a discussion board, receive technical assistance, and receive information disseminated by the center through the website.

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

Click here to enter text.

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

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

Click here to enter text.

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.

Users are required to agree to the Department's privacy policy on the page before using the website. The privacy policy is listed below.

PRIVACY POLICY

Privacy Policy is inherited from Department Privacy Policy and linked on the site. https://www2.ed.gov/notices/privacy/index.html

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

https://www2.ed.gov/notices/privacy/index.html

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?.

The LEAs and SEAs are required by the Department to submit the information.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

[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 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

Click here to enter text.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

SEA and LEA POCs have access to their profiles, which include first name, last name, email address and organization name.

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

Users must contact technical support to make changes to the information they provided.

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

Guidance for correcting information is provided on the website. Contact information for support is provided on the website.

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?

T4PA access is only available to authorized users. User access is managed T4PA Center program office. T4PA only supports communication using the the latest secured Transport Layer Security protocols. The system is independent; it does not collect data from other systems or share data with other systems. All personnel working with T4PA have to agree to established rules of behavior. Personnel in system administration and support roles must complete personnel background screening and complete additional training including role-based, incident response, and disaster recovery training.

Physical security is inherited and maintained by the AWS GovCloud. T4PA technical and administrative controls comply with the Federal Information Security Modernization Act requirements and with National Institute of Standards and Technology standards.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The system undergoes monthly scans and annual security assessment reviews, and is continuously monitored using endpoint protection tools.

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 T4PA system owner ensures that the information is used following stated practices in this PIA through several methods. One method is completing the Department Risk Management Framework process and receiving an Authority to Operate (ATO). Under this process, a variety of controls are assessed by an independent assessor to ensure the T4PA application and the data residing within are appropriately secured and protected. One-third of all NIST security controls are tested each year, and the entire system's security is re-evaluated regularly. The PIA is reviewed and update on an as-needed basis and at a minimum biennially. These methods 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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary and by not collecting any sensitive PII.

Role-based access controls are implemented to ensure access to data are restricted to authorized users only. Access to monitoring and auditing related documents are limited to Department employees with appropriately approved access authorization. User ID is displayed in discussion board posts, but no other PII data will not be posted to the T4PA Public Portal for any reason. Since users voluntarily decide what to share in discussion board posts, there is a possibility that PII could be exchanged through these posts.

The privacy risk associated with the system is minimal, as the system only stores SEA and LEA POC names, office email addresses, office phone numbers, user IDs, and passwords. The system only collects and maintains the minimal information needed for maintaining the login credentials.