



Privacy Impact Assessment (PIA)
for the

Teacher Shortage Areas Data Collection System (TSA)

January 5, 2022

For PIA Certification Updates Only: This PIA was reviewed on **December 10, 2021** by **Steven Sharma** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Freddie Cross
Contact Email: Freddie.Cross@ed.gov

System Owner

Name/Title: Freddie Cross
Principal Office: Freddie.Cross@ed.gov

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 Teacher Shortage Areas¹ (TSA) system consists of an informational website, data collection portal, and backend database that collects data from States and territories and presents data for public consumption on the teacher shortages in those respective areas. The data that are collected are intended for three purposes:

- To notify the public that States and schools may potentially hire academic administrators, licensed teachers, other educators and school faculty of specific disciplines/subject areas, grade levels, and/or geographic regions.
- To serve as a useful resource for recent graduates of Schools of Education and trained, experienced teaching professionals aspiring to serve school districts with shortages about potential opportunity areas in each State's and territory's Pre-Kindergarten through Grade 12 classrooms.
- To serve as a useful resource in the process of advising Federal student financial aid recipients of the potential to reduce, defer, or discharge student loan repayments by teaching in certain areas through the Teacher Education Assistance for College and Higher Education (TEACH) and Public Service Loan Forgiveness (PSLF) programs.


The public can access the TSA website and generate a "Teacher Shortage Areas Report" based on the following query variables: school year, state, subject matter, and discipline. These reports can be used for the purpose of complying with the TEACH Grant and PSLF requirements.

¹ According to 34 CFR 682.210(q)(8)(vii), "teacher shortage area" means "an area of specific grade, subject matter or discipline classification, or a geographic area in which the Secretary determines that there is an inadequate supply of elementary or secondary school teachers."

 **Generate TSA Reports - (Select criteria below as required)**

For historical Teacher Shortage Areas, please click on this link: [View PDF](#)

School Year:
 State:
 Subject Matter:
 Discipline:

 **Report**

School Year	State	County	School District	Geographic Region	Subject Matter	Discipline	Grades	Grades By Age
2021_2022	District of Columbia	-	-	-	Core Subjects	Elementary Education	K, 1, 2, 3, 4, 5, 6	Age above 5
2021_2022	District of Columbia	-	-	-	Mathematics	-	6, 7, 8, 9, 10, 11, 12	Age above 5

1.2. Describe the purpose for which the personally identifiable information (PII)² is collected, used, maintained or shared.

The system is designed to collect teacher shortage area data from States and territories. The individuals representing the States and territories who will enter the teacher shortage area data for their jurisdictions need to login using a username and password. They register for access by providing their name, email address, phone number (optional), and answers to security questions. This information is required for login information and to provide notices upon approval/disapproval of the application submission of teacher shortage area data.

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?

² The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. [OMB Circular A-130, page 33](#)

New PIA

While a PIA was not previously completed for TSA, a review of the system determined a PIA was required to accurately represent the PII collected by the 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.

Annual posting of the Nationwide Teacher Shortage Areas Listing designated by the Department of Education, as required under the following program regulations:

- 34 CFR 682.210(q) enables a borrower who had no outstanding Federal Family Education Loan (FFEL) Program loan on July 1, 1987 but who had an outstanding FFEL Program loan on July 1, 1993 to qualify for deferment of loan repayment under the Federal Stafford Program anytime within the life of the borrower's loan(s);
- 34 CFR 674.53(c) enables Federal Perkins Loan borrowers who are full time teachers of mathematics, science, foreign languages, bilingual education or any other field of expertise where the State educational agency determined there is a shortage of qualified teachers to qualify for cancellation of up to 100 percent of their loan; and
- 34 CFR 686.12(d) enables grant recipients to fulfill their teaching obligation under the Teacher Education Assistance for College and Higher Education (TEACH) Grant Program.

A State that desires to propose teacher shortage areas for designation must submit the information required under the program regulations for the following programs:

- Targeted teacher deferment for borrowers under the Family Federal Education Loan (FFEL) and Federal Supplemental Loans for Students (SLS) programs (34 CFR 682.210(q));
- Full-time teaching in fields of expertise, cancellation of up to 100 percent of their debt under the Federal Perkins Loan Program (34 CFR 674.53(c)); and
- Teaching obligation fulfillment for recipients under the Teacher Education Assistance for College and Higher Education (TEACH) Grant Program (34 CFR 686).

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

Information is retrieved by the following criteria: school year, State, subject matter, and discipline. The system does not retrieve information by an identifier.

2.3.

2.3.1. If the above answer is **YES**, this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).³ Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

N/A

2.3.2. 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 retrieved by the following criteria: School year, State, subject matter, discipline. The system does not retrieve by an identifier.

Records Management

³ 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>

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

- 2.4.** 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 Department shall submit a retention and disposition schedule that covers the records contained in this application to the National Archives and Records Administration (NARA) for review. The records will not be destroyed until such time as NARA approves said schedule.

- 2.5.** 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.

TSA collects the following PII from State and territory representatives and Department staff responsible for review and approval of reports of teacher shortage areas:

- Name
- Email address
- Phone number (optional)
- Answers to security questions

Once State and territory representatives are approved for access to TSA and have the ability to provide teacher shortage area data, there is an optional field to list the name of the Chief State School Officer (CSSO).

- 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 State and territory representative name, contact information, and optionally the name of the CSSO which is the minimum necessary to establish accounts and communicate with users.

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

The sources of PII collected are:

1. Individuals representing the States and territories who will provide teacher shortages areas for their States and territories, and
2. Department employees/contractors who are reviewers of the TSA.

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

TSA is a web-based system. PII is collected directly by the system from either the State and territory representatives responsible for data submission or the Department staff responsible for review and approval.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?⁴ Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The TSA program manager performs quality assurance reviews. Name, email address, phone numbers, and answers to security questions are the only PII collected and can be edited the by the individual user. This is currently a manual process where the TSA program manager logs into the system and reviews the registration requests to determine if the requester(s) are legitimately from a State and territory based on the domain of the email address of the requester.

Use

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

Both internal and external users log into the system using their email address as the User ID. Collection of user email address is necessary because users are sent emails throughout the application process with their approval status and if additional information is required.

⁴ Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

3.7. 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.

A privacy notice, as shown below, is drafted and will be posted on the collection website.

- 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

Authorities: A list of authorities can be found at [Teacher Shortage Areas \(TSA\)](#).

Information Collected: State and territory representatives name, work contact information, to include email address and phone number (optional).

Purpose: The purpose is to collect PII from individuals representing the States and territories who will provide teacher shortages areas for their States and territories.

Disclosures: The information will not be disclosed outside of the Office of Postsecondary Education.

Consequences of Failure to Provide information: Individuals representing the States and territories are obligated to provide the information identified on the [Registration](#) website to attain a TSA account. Failure to do so may result in not receiving a TSA account.

Additional information about this system can be found in the Privacy Impact Assessment.

- 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?

In order to gain access to the system, individuals have to provide the required PII. Individuals may wish not to provide certain information, but this can lead to not gaining 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?

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.⁵

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

⁵ 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.

5.8. 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?

Individuals have access to the system and can access their own information. Users log in and are restricted to editing their own information.

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

Individuals have access to the TSA and can edit/update their own information.

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

Users are notified via email and are asked to review their own information and, if needed, update/correct erroneous 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?

Data are encrypted by https protocol TLS 1.2. Physically, the application servers are secured within the FedRAMP-certified Microsoft Azure Platform as a service (PaaS) environment. Administratively, only system administrators authorized with “Internal” Role are allowed to see the PII.

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.

Vulnerability scans are conducted monthly to ensure the security on the network environment is protected. Annual security assessments are conducted as

self-assessments and independent assessments. Continuous monitoring occurs through the Department's Cybersecurity Risk Scorecard which provides a detailed view of the systems implementation of the required security and privacy controls and associated risk level of the implementation.

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 TSA provides mechanisms that enforce role-based access; there are no actions that can be taken by an anonymous person as registered user accounts are required for access. The general public is not granted access to the area of the website where PII is displayed or maintained.

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?

The main privacy risk associated with this system is unauthorized access to PII. In order to mitigate that risk, the system only collects the minimum necessary information to achieve the business purpose in order to limit risk if information were to be compromised. In addition, the system maintains auditing features that track authorized access to user accounts. These are the login and activity reports. The login report gives details about every access to the system. The activity report tracks all system changes made by authorized users. Records of users are audited on a quarterly basis by the Information Security Officer (ISO) to ensure that users are accurate. The TSA follows the Office of the Chief Information Officer (OCIO) policy, PR.AC 6: User Account Recertification. The system administrator may be directed to immediately remove any individuals who must no longer be granted access (i.e., in the event of an employee termination). In the event there is a point of contact (POC) change at an agency, the TSA staff will notify the system administrator who will then remove that person from the system access (within 24 hours of notification). The user accounts will have the passwords changed and the accounts are then disabled. After 90 days, those accounts are then deleted. There are other safeguards (e.g., physical, personnel, procedural, and environmental) that establish the extent that the system's design and implementation meet the set of OCIO-specified security requirements. The ATO granted using the

formal Department process that includes signatures by the Authorizing Official, ISO, Information System Security Officer (ISSO), and Senior Agency Official for Privacy. The ATO demonstrates that the information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.