Privacy Impact Assessment (PIA)

for the

Title II State Reporting System (T2SRS)

February 9, 2023

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: Terri Douglas/Information System Security Officer (ISSO)
Contact Email: Terri.Douglas@ed.gov

System Owner

Name/Title: Freddie Cross/Education Statistician
Principal Office: Office of Postsecondary Education (OPE)

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 Higher Education Act (HEA) Title II State Reporting System (T2SRS) supports the HEA Title II program, which gathers teacher quality data from the States in support of an annual report to Congress. Reports and data are made available to the public through the following website: https://title2.ed.gov. The data are collected by States from postsecondary institutions, alternative route teacher preparation programs, testing companies, and the States' own accountability systems. The data are reported by the 50 States, the District of Columbia, Puerto Rico, and other U.S. territories. No identifiable information is collected or reported on individual teachers.

Title II of HEA authorizes Federal grant programs that support the efforts of States, institutions of higher education (IHEs), and their school district partners to improve the recruitment, preparation, and support of new teachers. Title II also includes accountability measures in the form of reporting requirements for institutions and States on teacher preparation and licensing. The reported data include how institutions prepare teachers, what States require of individuals before they are allowed to teach, and how institutions and States are raising their standards for the teaching profession. These data measure the progress of teacher education programs and State efforts to improve teacher quality.

The T2SRS includes the public website, a State data entry application, an IHE data entry application, a data mining and reporting ("data tools") application, a project file share (for States to upload relevant documentation), and associated development and staging/testing environments. State Education Agencies (SEAs) and IHE administrators request access to the reporting website by calling the HEA Title II help desk and providing the information identified in question 3.1 to the help desk in order to create an account for access. The help desk sends a yearly email to the SEA and IHE administrators to change their passwords. This process allows for the help desk to identify if there are any needed changes for who needs access to the reporting website.

Data flow through the system follows the path defined in the Title II reporting requirements. Data flow from the various education institutions to the SEAs using the

IHE data entry application. The States then assemble and submit their data to the Department using the State data entry application of the T2SRS. Some data are submitted as files which can be uploaded or emailed to Department project staff for uploading. Uploaded files are processed to extract the data and import them into the T2SRS database. Data are also entered and edited using extensive online forms, which make up the majority of the data entry applications. Project staff also edit the data using the data entry applications.

Business contact information is collected for a primary contact at the SEAs for use in administering the collection and reporting of data. The business contact can choose to display or not to display this contact information on the public website. Business contact information is also collected from the educational institutions, but this information is not displayed on the public website.

After the State data are uploaded, data are extracted from the database, analyzed, and assembled into the tables and text that are used in the annual report and released to the public. Once the annual report has been created, it is then submitted to Congress. The text, tables, reports, and files are then made available through the public website.

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

SEAs and IHEs submit primary contact name and work information for administration of the project. The SEA may choose to display their contact information on the public website; the information from IHEs is not displayed on the public website. No individual teacher information is collected or maintained in this system.

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?

Updated PIA

The PIA is being updated as part of the required biennial review.

[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 system operated by the agency or by a contractor?

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

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 data are collected and used pursuant to the authority in Title II (Sections 205 through 208) of the Higher Education Act. The Higher Education Opportunity Act (Public Law 110-315) (HEOA) was enacted on August 14, 2008, and reauthorizes the HEA of 1965, as amended. The HEA Title II program gathers teacher quality data from the States in support of an annual report to Congress and authorizes new Federal grant programs that support the efforts of States, IHEs, and their school district partners to improve the recruitment, preparation, and support of new teachers.

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

[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

maintained in a system of records, or the information is not maintained by the Department, etc.

□ N/A

Information is not retrieved using an individual 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.

The records schedules for T2SRS are:

- **State and Institutional Records**: No data has been purged. (The system currently holds 9 years of data.): ED 065, Reports to Congress and/or the President, item b: Work Files: **Temporary**. Cut off file annually upon transmittal to Congress or the President. Delete/Destroy 5 years after cutoff after approval from the Department Information Management Branch (IMB) / Office of General Counsel (OGC).
- **Final Reports to Congress:** ED 065, Reports to Congress and/or the President, item a: Final Report. **Permanent.** Cut off annually. Transfer to National Archives 5 years after cutoff with assistance from IMB.
- **Activity logs:** General Records Schedule (GRS) 3.1, item 020: Information technology operations and maintenance records. **Temporary**. Cutoff annually, destroy after 3 years, as per GRS.
- **Ticketing requests:** GRS 6.5, item 010: Public customer service operations records. **Temporary.** Destroy 1 year after resolved, or when no longer needed for business use.

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

Yes

3. Characterization and Use of Information

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.

The information collected is business contact information for contacts at SEAs and IHEs. The information collected is name, title, organization/institution name, business address of organization/institution, business phone and fax, business email address, and T2SRS password. The SEA may choose to display, or not to display, the contact information on the public website; the information for IHEs is not displayed.

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

Yes

T2SRS collects only the minimum information necessary to administer the Title II State reporting process. Contact information is needed to communicate with the SEAs if any questions come up during the reporting process. In addition, T2SRS uses this information to allow for SEA and IHE personnel to access the T2SRS website in order to submit data. No information is collected that is not required to achieve these purposes. If individuals do not provide the required PII, it may prevent from an account to be created in order for SEAs and IHE to access the T2SRS website.

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

PII is submitted by the SEA and IHE staff.

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

Information is collected via telephone when the SEA or IHE contacts contact the T2SRS help desk to establish an account for access. Once the contacts log in to the T2SRS system, they are presented with a work contact information collection screen, which collects additional information and allows previously submitted contact information to be updated.

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.

SEAs and IHEs are responsible for ensuring the accuracy of their own information; if incorrect information is submitted, individuals will not receive communications from the Department. Errors are identified if the Department is unable to contact the SEAs and/or IHEs. The SEAs and IHEs are required to certify or provide updated contact information on an annual basis.

Use

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

SEAs and IHEs submit primary contact name and work contact information for project administrators in order for the Department to contact the SEAs and/or IHEs, if needed. SEAs may also choose to display their information on the public website for use by the general public.

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.

Public notice is provided through the publication of this PIA. SEA and IHE administrators request access to the reporting website by calling the HEA Title II help desk, providing the information identified in question 3.1 to the help desk in order to create an account for access. Since information collection is done orally, notice is provided to the SEA and IHE administrators while the collection is happening through calling the T2SRS help desk.

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

Under the authority in Title II (Sections 205 through 208) of the Higher Education Act, the U.S. Department of Education is collecting your personally identifiable information in order to create an account for access to the T2SRS system. You may opt-in to display your contact information on the public facing T2SRS website but doing so is not mandatory. Failure to provide any of the requested information may result in an account not being created for T2SRS access.

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 information is provided by the SEAs and IHEs to provide work contact information for administrators of the project. If individuals do not provide the required PII, it may prevent from an account to be created in order for SEAs and IHE to access the T2SRS website. The SEAs can also choose to display, or not to display, the information to users of the public website. The SEAs are provided with a simple checkbox on the work contact information collection screen to indicate “Public Contact.” If checked, the contact information is displayed on the public website. This indication can be changed at any time by the SEAs through the T2SRS.

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.

Yes

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

If an SEA opts in, work contact information for the primary contact will be displayed on the public website.

[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.

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

□ N/A

The contact information is shared for use by individuals who access the public website. This information is shared for the purpose of allowing individuals from the public to contact the SEA administrators if there are any questions related to the data for their particular State.

5.6. Is the sharing with the external entities authorized?

□ N/A

Yes

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

The work contact information is displayed on the public website.

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

No

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

□ N/A

No

6. Redress

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

The SEAs and IHEs have access to their information through the website and may update their information at any time.

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

The SEAs and IHEs have access to their information through the website and may update their information at any time.

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

The SEAs and IHEs have access to and may update their information at any time. No explicit instructions or procedures are provided to the SEAs or IHEs for correcting their information. Data are collected and reported by the SEAs and IHEs through the T2SRS on an annual basis, and it is incumbent on the agencies/institutions to ensure their information is correct.

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?

T2SRS is hosted on the IBM SmartCloud for Government cloud computing platform. T2SRS only supports secure communication protocols for both T2SRS users and the T2SRS application/website. All personnel working with the T2SRS agree to established rules of behavior. Personnel in system administration and support roles must successfully complete personnel background screening for moderate risk and complete additional training including role-based, incident response, and disaster recovery training.

Access to the system is limited to authorized Department users responsible for reviewing submissions. Authorized personnel include Department employees and contractors. The system limits data access to Department employees and contractors on a “need to know” basis and controls individual users’ ability to access and alter records within the system. Department employees and contractors are also required to complete security and privacy awareness training on an annual basis.

The T2SRS Information System Owner (ISO) is responsible for daily operational oversight and management of the system’s security and privacy controls and ensuring to the greatest possible extent that the data are properly managed and that all access to the data has been granted in a secure and auditable manner. The T2SRS ISO is responsible for ensuring that any loss, compromise, unauthorized access, or unauthorized disclosure of PII is reported to the Department’s Office of the Chief Information Officer, the Student Privacy Policy Office, and the appropriate Department officials in accordance with Federal policy and established Department procedures.

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.

T2SRS is entered in the Department’s Cyber Security Assessment and Management (CSAM) system. The CSAM system is the cybersecurity tool requiring monitoring, testing, and compliance to DHS, OMB, and Department cybersecurity mandates on a continuous basis. T2SRS is required to obtain and maintain an Authorization to Operate (ATO). This process includes a quarterly assessment of security and privacy controls, through the Department's Ongoing Security Assessment (OSA) program, and produces Plans of Actions and Milestones to ensure any deficiencies are remediated.

As part of the ATO granted by the Security Authorization Program, T2SRS will be required to comply with both the current version of NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring for Federal Information Systems and organizations and the Department's Information Security Continuous Monitoring Roadmap.

Examples of testing or evaluation include weekly vulnerability scans and mitigation of vulnerabilities within the times specified by the Department. Annual application scans, and mitigation of vulnerabilities within specified times, are also performed. These application scans are performed more frequently depending on programming updates to the application/site. The Department also performs annual assessments on applicable security and privacy controls.

8. Auditing and Accountability

How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The T2SRS system owner ensures that the information is used in accordance with stated practices in this PIA through several methods. One method is completing the Department Risk Management Framework process and receiving an ATO. Under this process a variety of controls are assessed by an independent assessor to ensure the T2SRS application and the data residing within are appropriately secured and protected. One-third of all controls are tested each year and the entire system security is reevaluated every three years. The PIA is reviewed and updated on an as needed basis and at a minimum, every 2 years. These methods together with regular communication with the T2SRS users ensures that the information is used within the stated practices outlined in this PIA.

8.1. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.2. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with T2SRS 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 identity theft, embarrassment, or financial loss. 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 per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.