Privacy Impact Assessment (PIA)
for the

National Technical Assistance Center for the Education of
Delinquent Children and Youth (NDTAC)
May 17, 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: Felicia Goss
Contact Email: felicia.goss@ed.gov

System Owner

Name/Title: Metasebia Belachew
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 National Evaluation and Technical Assistance Center for the Education of Children and Youth Who Are Neglected, Delinquent, or At Risk (NDTAC) is the U.S. Department of Education (Department)-funded technical assistance center that supports the implementation of the Elementary and Secondary Education Act of 1965 Title I, Part D (Title I, Part D) grant program. NDTAC is a website that uses a MySQL database to house website data. The NDTAC website provides visitors with information about the Title I, Part D grant and other related programs, including links to relevant Federal resources (including the statutory text and non-regulatory guidance authored by the Department) and NDTAC-produced technical assistance resources designed to support grantee implementation (including tip sheets, research publications, and training materials). The NDTAC website publishes data about students classified as neglected, delinquent or at risk and includes resources to support grantees in collecting, reporting, and analyzing student data, activities which are all required by the Department and statute. The data are provided on the NDTAC website in multiple ways, including data aggregated at the national level and data that are state-specific. NDTAC maintains a help line (via both email and phone) for use by grantees, stakeholders, and students and families of neglected, delinquent, and at-risk children and youth, and the center's website provides information about contacting the NDTAC staff directly.

   Primary users of the system are state education agencies (SEAs), which receive Title I, Part D program grants from the Department. Secondary users of the site include entities that receive subgrants from SEAs, as well as school-based personnel, service providers, parents, students, and other interested stakeholders. The system does not collect any information from users, nor does it allow logins to the site. The website displays contact information for state Title I, Part D education coordinators. The system is hosted in the Amazon Web Services (AWS) hosting environment, a shared service hosting provider for the Department.

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

Information collected is used to disseminate information about state coordinators for the education of children and youth classified as neglected, delinquent, or at-risk. The Department allocates Title I, Part D funding annually to states based on a state's proportion of the Title I, Part D Federal allocation. States must subgrant funds by formula to LEAs within the state to be used for program implementation at the district level. The system also collects NDTAC staff contact information so that system users may contact them. Information provided on the website allows the users to contact the state coordinators and NDTAC staff personnel.

1.3. Is this a new system, or one that is currently in operation?

New System

1.4. Is this PIA new, or is it updating a previous version?

New PIA

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 Title I, Part D of the Elementary and Secondary Education Act (20 U.S.C. 6301 et seq.), as amended. The program regulations are in the U.S. Code of Federal Regulations at 34 CFR 222. These authorities allow for the establishment and maintenance of the program, including determining local education agency (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

---

[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

business use. Executive Order 13556 (2010), is federal non-classified information that must be safeguarded by implementing a uniform set of requirements and information security controls directed at securing sensitive government information.

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 system collects the following information from state neglected and delinquent education coordinators.
- Name of the coordinator
- Organization
- Organization address
- Organization phone number
- Organization fax
- Organization email

The system collects the following information from NDTAC staff:
- Name
- Email address
- Phone number

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

Yes

The names and contact information of state coordinators and NDTAC staff are used to allow visitors to the website to contact them. Only the minimum contact information necessary is collected that will allow users to identify the relevant coordinators and staff and then contact them.

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

State coordinator information is provided by state coordinating offices. NDTAC staff information is provided by NDTAC 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.)?

Program officers directly contact state coordinating offices to collect information on state coordinators and add it to the webpage. NDTAC staff send contact information directly to the website administrators to be posted. This information is reviewed on an annual basis or when staff turnover occurs and NDTAC staff are notified of the change.

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 state coordinating offices to verify the contacts as required for managing a Title I, Part D program. The program office is responsible for making updates and ensuring the data on the website are correct. NDTAC staff send the information directly. As it is their own contact information, it is likely to be correct.

Use

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

Coordinating office and point of contact information for both state coordinators and NDTAC staff is posted on the website to allow coordination and collaboration with local agencies and to assist in providing comprehensive services to neglected, delinquent, and at-risk children and youths and their families.

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?

---

[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.

☑ 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

        3.8.1. 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.

Website visitors do not submit any information using the website. There is no "User's" repository or user specific accounts stored within the system.
NDTAC staff and state coordinators provide their contact information explicitly so that it can be publicly displayed. They are notified of this purpose when the information is collected as specified under the contract between the Department and the state in question. Additionally, this Privacy Impact Assessment provides notice.

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

Click here to enter text.

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 coordinating officers are required to submit the information as a requisite for taking part in the program. NDTAC staff voluntarily provide this information so that they can be contacted to provide assistance and 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

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

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.

---

[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.

5.11. 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?

State coordinators and NDTAC staff can access the website to view their information.

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

State coordinators must contact the Federal program officer to make changes to the information they provided. NDTAC staff may contact the website administrator or NDTAC Help Desk (link and telephone number) to report an issue with the website information.

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

Federal program officer will notify the state coordinator by email about the procedures for correcting their information as specified under the contractual arrangement between the Department and the state in question. NDTAC staff provide the information directly to the website administrators, and so would be aware to reach out if changes are needed.

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?

User access is managed by NDTAC program office. NDTAC only supports communication using the latest secured Transport Layer Security protocols. The system does not collect data from other systems or share data with other systems. All personnel working with NDTAC 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 Support System. NDTAC technical and administrative controls comply with the Federal Information Security Modernization Act requirements and with National Institute of Standards and Technology (NIST) 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 NDTAC system owner ensures that the information is used following stated practices in this PIA through several methods. One method is completing the Department's Risk Management Framework process and receiving an authorization to operate (ATO). Under this process, a variety of controls are assessed by an independent assessor to ensure the NDTAC 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 every three years. The PIA is reviewed and updated 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 to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. The privacy risk associated with the system is minimal, as the system only collects the state coordinator names, office email addresses, office phone numbers and address and NDTAC staff name and phone numbers. This is not sensitive PII, and in fact, is intended to be public. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary. All users have the guest role, which provides anonymous access to all pages on the website. Access to monitoring and auditing related documents are limited to Department employees with appropriately approved access authorization.