



Privacy Impact Assessment (PIA)
for the

Migrant Student Information Exchange

February 26, 2021

For PIA Certification Updates Only: This PIA was reviewed on by 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: Patricia Meyertholen
Principal Office: Office of Elementary & Secondary Education (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 Migrant Student Information Exchange (MSIX) supports the Migrant Education Program (MEP), which is administered by the Office of Migrant Education (OME) under the Office of Elementary and Secondary Education (OESE). The MEP supports state educational agencies (SEAs) by providing funding to help SEAs establish or improve educational programs for migratory students. MSIX has been developed to provide an effective method for electronically exchanging migrant student records amongst states; and, to determine an accurate count of the number of migratory children in each state. As such, MSIX provides a means for states to coordinate information sharing for the migratory student community.

Additionally, the Secretary is authorized to use MSIX data for the purpose of providing stakeholders with census data and statistics on the national migratory population and to meet other reporting requirements related to the national migratory child population. Authorized users of MSIX include SEA and local education agency (LEA) officials, OME staff, and MSIX contractor staff.

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

The information in MSIX is being collected to enhance the continuity of educational and health services for migratory children by providing a mechanism for all states to exchange educational and health related information on migratory children who move within states and/or from state to state due to their migratory lifestyle. The use of MSIX improves both the timeliness of school enrollments and the appropriateness of grade and course placements and reduces incidences of unnecessary immunizations of migratory children. Further, MSIX facilitates the accrual of course credits for migratory children in secondary school by providing accurate academic information on the student's course history and academic progress toward the goal of high school graduation or high school equivalency in a timely manner. MSIX and records within MSIX are to be used for the

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](#)

purposes of facilitating a migratory child's: (i) participation in the MEP; (ii) enrollment in school; (iii) grade or course placement; and (iv) credit accrual.

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

This PIA is being updated as part of its regular biennial schedule.

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.

Section 1308(b) of the ESEA authorizes the U.S. Department of Education (ED) to operate and maintain a migrant student information exchange database system. Further, 34 CFR §200.85 outlines the responsibilities of SEAs for the electronic exchange through MSIX of specified educational and health information of migratory children and regulates the collection and use of MSIX data. Information Collection Notice Office of Management and Budget (OMB) Control Number 1810-0683 permits the collection of minimum data elements (MDEs) for the stated purposes. Information Collection Notice OMB Control Number 1810-0686 for the MSIX User Application Form permits the collection of authorized user information.

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?

Yes

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

The system is covered under the System of Record Notice Migrant Student Information Exchange (MSIX), SORN (18-14-04) published in the Federal Register on July 10, 2019.

<https://www.federalregister.gov/documents/2019/07/10/2019-14686/privacy-act-of-1974-system-of-records--migrant-student-information-exchange>

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

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.

Records created and received by MSIX will not be destroyed until an appropriate Departmental records disposition schedule is developed and approved by the National Archives and Records Administration. The Department's Records Officer is currently processing changes to records retention schedules, which will impact MSIX.

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

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.

MSIX data requirements are specified in the Minimum Data Elements (MDE) document developed by ED and approved by OMB. Information collected includes: Name, date of birth, personal identification numbers assigned by the States and the Department, parents' or guardians' names, school enrollment data, school contact information, assessment data, medical alert indicator, and other educational and health data necessary for accurate and timely school enrollment, grade and course placement, and accrual of course credits.

In order to gain access as an authorized user, MSIX collects the individual's full name, work email, work address, work phone number, job title, and role assigned.

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

Yes

All information collected is used for the purpose of the collection; to enhance the continuity of educational and health services for migratory children, and to administer this program. Only the minimum information necessary is collected.

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

As owners of their data, the SEAs are the authoritative source of all information contained in the MSIX system. All data is submitted by SEAs through their individual operated and owned migrant-specific databases. The SEAs are responsible for collecting all information directly from parents and/or students. Parent includes legal guardian or other person standing in loco parentis, such as a grandparent, stepparent or other relative with whom the child lives or temporarily resides, or a person who is legally responsible for the welfare of the child. Direct data entry or data editing by individual users is not

permitted in MSIX. MSIX receives encrypted XML file feeds from SEA-operated systems, which are considered the authoritative data source for the records. The SEA and its sub-grantees may collect this information directly from parents and students on paper or electronic forms. MSIX ingests files transmitted securely through established channels and consolidates the records into a single national information exchange system.

Information collected to authorize access to MSIX is collected directly from the MEP State Director or designee via an account application form.

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

MSIX receives encrypted XML file feeds from SEA-operated systems, which are considered the authoritative data source for the records. The SEA and its sub-grantees may collect this information directly from parents and students on paper or electronic forms. MSIX ingests files transmitted securely through established channels and consolidates the records into a single national information exchange system. The SEAs do not have the ability to enter their data directly into the MSIX database. Information collected regarding authorized user access is collected on a paper or electronic application which has been approved by OMB.

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 information contained in MSIX is reviewed for accuracy and timeliness through a variety of methods. Because SEAs are the authoritative sources of data, SEA personnel are responsible for performing data checks at the SEA level as documented in the MSIX interface requirements specification guide. File integrity checks are conducted in the file ingestion process, and records or files that do not meet file specification requirements are rejected. Error reports are sent back to the source SEA for data correction. After the data are loaded into MSIX, data quality and validity reports are available to the SEA designated data administrators.

Use

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

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.

The information is used to facilitate the timely enrollment, grade and course placement, accrual of secondary credit leading to graduation, MEP participation as well as to produce national statistics on the population of migratory children.

The information in MSIX is being collected to enhance the continuity of educational and health services for migratory children whose educational and academic progress is often interrupted due to frequent moves as well as their participation in the MEP. The use of MSIX improves the timeliness of school enrollments, the appropriateness of grade and course placements, and reduces incidences of unnecessary immunizations of migratory children. Further, MSIX facilitates a migratory child's participation in the MEP through the identification and recruitment process as well as the accrual of course credits for migratory children in secondary school by providing accurate academic information on the student's course history and academic progress. By allowing participating SEAs to electronically exchange academic history and health information for migratory children, the students are enrolled in the MEP and placed in grades, programs, services and coursework nationwide without delay.

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

[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.

SEAs are responsible for following their State laws for providing notice about the collection of PII and ensuring parents and guardians are aware of their privacy rights and give consent for their child to participate in the MEP, which includes submission of the child's information to MSIX through the MDEs. Participation in the MEP is voluntary, and parent's may choose for their children to not participate.

The MSIX system does not provide direct notice to individuals about the collection of their PII in MSIX prior to its collection because the MSIX system does not collect such information directly from the affected individuals, but rather from participating SEAs. Section 1308 of the ESEA does not include specific provisions addressing the protection of education records as it relates to the MSIX information system, and, as mentioned above, the protections in 99.35(b) regarding re-disclosure do not apply to records in the MSIX. However, the Privacy Act applies to MSIX, and the department has published a system of records notice (SORN) to cover this system of records, which includes routine uses that indicate what disclosures from MSIX can be made without the child's or his/her parent's consent. See 84 FR 32895 pages 32895-32899 (July 10, 2019). FERPA (Section 444 of the General Education Provisions Act) establishes the rights of parents to examine and question the content of their children's school records and restricts the transfer of school records without parental permission. It applies to any local educational agency that receives Federal funds. One exception to the restriction on the transfer of school records without parental consent is if the local educational agency transfers the records to other school officials within the agency (whom the agency has determined to have legitimate educational interests) or to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll. (See 34 CFR 99.31.) This exception applies only if the local operating agency notifies parents annually of this policy. This exception does not apply to SEAs that maintain education records in a paper or electronic format and wish to transfer such records to another State or local operating agency. In this case, the SEA must obtain parental consent

before it transfers the records. Under FERPA, parents have the right to be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record. SEAs are responsible for collecting and maintaining parental consent as required under FERPA.

- 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

PRIVACY ACT INFORMATION - Found on the MSIX log-in screen

You must read the statement below and click "Continue" to access the Department of Education's MSIX website. Some users may need to scroll to the bottom of the screen to see the "Continue" button. This is a United States Department of Education computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. This system contains personal information protected under the provisions of the Privacy Act of 1974, 5 U.S.C. § 552a - - as amended. Violations of the provisions of the provisions of the Act may subject the offender to criminal penalties.

- 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?

SEAs are responsible for collecting, validating and submitting source data into MSIX. The opportunity for individuals to consent to uses, decline to provide information or opt out of MSIX is provided by the SEA at the time of the initial interview to determine eligibility for the MEP. If the individual does not consent to uses, declines to provide information or opts out of MSIX, the Certificate of Eligibility (COE) which records a child's eligibility for the MEP cannot be completed; therefore, the child could not be counted as an eligible migrant child by the SEA. MSIX regulations require that all eligible migratory children's records be uploaded to MSIX, therefore, parents of migratory children who opt out or otherwise do not have an approved COE would not be eligible for the program and would not be submitted to MSIX.

- 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

Consolidated Student Records and all MDEs collected from participating SEAs receiving MEP Grants are available for search by all other participating SEAs. The SEAs may authorize access to MSIX to MEP-funded local operating agencies (LOAs) and LEAs with migratory children. The SEA may authorize access only for the purposes of school enrollment, grade and course placement, accrual of high school credits, and participation in the MEP for eligible migratory children. Information may be shared with school officials as authorized by the SEA or LEA.

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.

All SEAs submitting and accessing the data in MSIX has and maintains a Memorandum of Understanding (MOU) that defines the roles and responsibilities for use of MSIX and an Interconnection Security Agreement (ISA) that defines the technical requirements for maintaining a secure data connection. Through the MOU, each SEA agrees that the MDEs received through MSIX and records within MSIX will only be used for the purposes set forth in Question 1.2 above.

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

N/A

ED may disclose information to the external entities listed in Section 5.5 in alignment with the purposes as stated in Question 1.2 above.

5.7. Is the sharing with the external entities authorized?

N/A

Yes

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

N/A

Yes

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

N/A

Information in MSIX is accessed by authorized users who have the credentials to access the MSIX system. Users are authorized by the State MEP Director and must agree to the MSIX Rules of Behavior. Participating States act in accordance with the terms outlined in the MSIX Interconnection Security Agreement (ISA). Both the MSIX Rules of Behavior and the ISA include conditions under which MSIX information may be shared. For further information, please reference the Routine Uses of Records Maintained in the System Including Categories of Users and the Purposes of Such Uses section in the referenced MSIX SORN (18-14-04).

SEAs, LEAs, and other MEP LOAs share the information in MSIX with school personnel, including, but not limited to, guidance counselors, registrars and MEP-funded staff to facilitate school enrollment, grade placement, accrual of secondary credits toward graduation, and participation in the MEP of eligible migratory children. Available information includes migrant student enrollment and demographic information, course history, assessments, medical alerts, availability of immunization

records and other information, e.g., whether the student is an English Learner or should have priority for services.

- 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

Yes

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

N/A

Yes

6. Redress

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

Individuals can gain access to their information by requesting their record from their SEA, LEA, or participating MEP LOA. Further information on how individuals can access their information held by the Department can be found in the MSIX SORN (18-14-04).

<https://www.govinfo.gov/content/pkg/FR-2019-07-10/pdf/2019-14686.pdf>

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

Individuals can seek to correct to their information by requesting their record from their SEAs, LEAs, and MEP LOAs as well as from the Office of Migrant Education at the U.S. Department of Education. Further information on how individuals can correct their information held by the Department can be found in the MSIX SORN (18-14-04).

<https://www.govinfo.gov/content/pkg/FR-2019-07-10/pdf/2019-14686.pdf>

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

Individuals are notified of the procedures for correcting their information by the posting of this PIA and through the publication of the SORN.

<https://www.govinfo.gov/content/pkg/FR-2019-07-10/pdf/2019-14686.pdf>

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?

MSIX access is only available to authorized users. User access is managed by OME and the SEA. MSIX only supports secure communication protocols for both MSIX users and SEA interconnected systems. All personnel working with MSIX must agree to established rules of behavior and complete annual basic security awareness training. Personnel in system administration and support roles must successfully complete personnel background screening for moderate risk positions and complete additional training including role-based, incident response, and disaster recovery training. MSIX technical and administrative controls comply with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards and guidelines. The MSIX Data Management Plan is an administrative control including policies and procedures to handle and protect all information, including PII. In addition, the systems within MSIX are configured to log user access and actions. Logs are reviewed monthly and as needed.

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.

MSIX is authorized for operation in accordance with the Department's Security Assessment and Authorization (SA&A) Program. As part of the Authority to Operate (ATO) granted by the SA&A Program, MSIX is required to comply with both the current version of NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and organizations and the Department's Information Security Continuous Monitoring Roadmap. Examples of testing or evaluation include running vulnerability scans and mitigating vulnerabilities within the times specified by the Department in addition to performing annual self-assessments on one-third of the applicable security controls.

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 ensures that the information is used in accordance with stated practices in this PIA through several methods. The first method is by completing the ED SA&A process and receiving an ATO. Under this process a variety of security controls are assessed by an independent assessor to ensure the MSIX application and the data residing within are appropriately secured and protected. One-third of all security controls are tested each year and the entire system security is re-evaluated every three years. The second method is by requiring all MSIX users to complete annual security and privacy awareness training. Lastly, the system prompts users to read and acknowledge the MSIX Rules of Behavior at their first login after account creation and every 12 months thereafter. The PIA is reviewed and updated on an as needed basis and at a minimum every two years. In addition, the OMB information collection authorizations are reviewed and updated on a federally mandated schedule. These methods together with regular communication with the MSIX contractor team and users ensures 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.

The primary risks posed by the collection and storage of information in MSIX are associated with, and flow from, the potential loss of control of this information, including unauthorized access, alteration, or dissemination. To mitigate the risks detailed below, MSIX has implemented several safeguards including those administrative, technical, and physical safeguards addressed in Section 7.3.

One key risk is the potential for unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud. The risk is mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.

Another privacy risk could entail human error related to database management. This risk is managed through the application of several controls identified in the system security plan (access controls, configuration management, audit and accounting, identification and authorization, boundary controls, etc.).

Additional privacy risks are mitigated as the system collects only the minimum PII necessary to achieve the authorized program purpose. Additionally, the information collected is considered to be fairly low risk, as it is only name and work contact information and does not include any elements that have been identified as sensitive.