Privacy Impact Assessment (PIA)
for the

Migrant Student Information Exchange
December 19, 2023

For PIA Certification Updates Only: This PIA was reviewed on **Date** by **Enter Name** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Anu Bezwada
Contact Email: Anu.Bezwada@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 who move within States or between States due to their migratory lifestyle. 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. Authorized users of MSIX include SEA and local education agency (LEA) officials, OME staff, and MSIX contractor staff. MSIX provides a means for States to coordinate information sharing for the migrant student community, facilitating migrant students' participation in the MEP, enrollment in school, grade or course placement, and credit accrual.

Additionally, the Secretary of Education is authorized to use MSIX data for the purpose of providing stakeholders with census data, statistics, and other reporting requirements related to the national migrant population. Authorized users of MSIX include SEA and local education agency (LEA) officials, OME staff, and MSIX contractor staff. To access MSIX, these authorized users are required to register for accounts, which are verified by U.S. Department of Education (Department) 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 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. MSIX improves both the timeliness of school enrollments and the appropriateness of grade and course placements and reduces incidences of redundant immunizations of migratory children. Further, MSIX ensures the accuracy of migratory children's secondary school course credit accural by maintaining information on each student's course history and

[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

academic progress toward the goal of secondary school graduation or equivalency.

Migrant student data contained in MSIX is collected by SEAs, who collect the information directly from parents/guardians and/or students. SEAs submit this information to MSIX as encrypted XML files; MSIX consolidates the information received through these XML files into a concentrated national information exchange. Once information is collected by MSIX, each migrant child's record is assigned a unique, system-generated identification number referred to as an MSIX ID.

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 reviewed as part of the biennial review process.

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 Elementary and Secondary Education Act (ESEA) authorizes the Department 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.

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/

The SORN, titled "Migrant Student Information Exchange (MSIX)," 18-14-04, 84 FR 32895, was published in the Federal Register on July 10, 2019.

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

Click here to enter text.

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 has submitted changes to the MSIX records retention schedule under NARA Electronic Records Archives case number DAA-0441-2022-0001-0003, which will impact MSIX records retention by extending retention to 30 years after final student record activity.

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

[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

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.

Information collected about migratory students includes name, date of birth, personal identification numbers assigned by States and the Department (including MSIX ID), parents' or guardians' names, school enrollment data, school phone number and address, academic assessment test scores, course history and grades, medical alert indicators in the event that the child has a chronic or acute health condition, immunization records, and other educational data necessary for accurate and timely school enrollment, grade and course placement, and accrual of course credits.

MSIX also collects authorized users' (including Federal employees, contractors, and SEA and LEA representatives) full names, work email addresses, work addresses, work phone numbers, job titles, roles, usernames and passwords for account creation.

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

Yes

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

All data is submitted to MSIX by SEAs, which is stored in their respective systems. The SEAs are responsible for collecting all information directly from parents and/or students. The SEA and its sub-grantees may collect this information directly from parents and students on paper or electronic forms.

Information collected to authorize access to MSIX is collected directly from the MEP State Director or designee via a standardized account application form. The MEP State Director is the primary point of contact for each State's MEP.

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

The SEA collects information directly from parents and students on paper or electronic forms and the information is then entered into various SEA-operated systems. MSIX

receives encrypted XML file feeds from SEA-operated systems at regular, automatic intervals via a secure connection to SEA systems. MSIX ingests files transmitted securely through established channels and consolidates the records into a single national information exchange system.

Information collected regarding authorized user access is collected on a paper or electronic application which has been approved by the Office of Management and Budget (OMB). The information collected for user access is then manually entered into the MSIX system by User Administrators for the purpose of creating the applicant's user account. User Administrators establish and manage user accounts for users in their State.

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 through a variety of methods. Because SEAs are the sources of data, SEA personnel are responsible for performing data checks at the SEA level. File integrity checks are conducted in the file ingestion process. 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 administrators.

Use

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

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

The information in MSIX is 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. MSIX facilitates a migratory child's participation in the MEP as well as the accrual of course credits for migratory children in secondary school by providing accurate 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, students are able to be enrolled in the MEP and placed in appropriate grades, programs, services, and coursework nationwide without delay.

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

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. 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.

Notice is provided in the MSIX SORN. Outside of the SORN, the MSIX system does not provide direct notice to individuals about the collection of their PII prior to its collection because the MSIX system does not collect such information directly from the

affected individuals, but rather from participating SEAs. SEAs, as the initial point of collection, are responsible 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. Participation in the MEP is voluntary, and parents may choose for their children to not participate.

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?

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. While participation in the MEP is voluntary, information must be submitted to MSIX via SEAs to be eligible for participation.

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.

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

All information collected from SEAs is available for search in MSIX by all other participating SEAs. The SEAs may authorize MSIX access to MEP-funded programs with migratory children by having prospective users fill out the MSIX user application form and creating accounts for them to access MSIX, if allowable. The SEA may authorize access only for the purposes of school enrollment, grade and course placement, accrual of secondary 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.

SEAs and LEAs 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. This sharing occurs by granting access to the MSIX system via the MSIX user application and creation of an MSIX account when allowable. Available information includes migrant student enrollment and demographic information, course history, assessments, medical alerts, availability of immunization records and other information as described above.

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

☐ N/A

The Department may disclose information to the external entities listed in Section 5.5 to facilitate school enrollment, grade placement, accrual of secondary credits toward graduation, and participation in the MEP of eligible migratory children.

5.7. Is the sharing with the external entities authorized?

☐ N/A

[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.

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

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.

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

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 or LEA, as well as from the Department.

If an individual wishes to gain access to their record in this system of records, they must contact the system manager at the address listed under SYSTEM MANAGER(S) in the SORN referenced in question 2.2.1. They must provide necessary particulars such as name, date of birth, and any other identifying information requested by the Department

while processing the request to distinguish between individuals with the same name. The request must meet the requirements of regulations in 34 CFR 5b.5, including proof of identity.

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

Individuals can seek to correct their information by requesting their record from their SEAs and LEAs, as well as from the Department.

If an individual wishes to contest or change the content of a record regarding them in the system of records, contact the system manager at the address listed under SYSTEM MANAGER(S) in the SORN referenced in question 2.2.1. The request must meet the requirements of regulations in 34 CFR 5b.7.

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.

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?

The system employs a full suite of administrative, technical, and physical safeguards to protect information based on Federal requirements pursuant to National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 (SP 800-53) and best practices. The system has been evaluated against the SP 800-53 moderate profile with FedRAMP cloud enhancements. Safeguards include password-based and two-factor authentication, role-based access control, data encryption, and physical data center security for candidates, contractors, and Federal employees.

Security protocols for this system meet all required security standards. Physical access to the Department site where this system is maintained is controlled and monitored by security personnel who check each individual entering the building for their employee or visitor badge.

The system limits access to users on a "need to know" basis and controls users' ability to access and alter records within the system. Access to various parts of the system is restricted based on user role and level of authorization. In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every Department system must receive a signed Authorization to Operate (ATO) from a designated Department official. The ATO process includes a rigorous assessment of security and privacy controls, plans of actions and milestones (POA&Ms) to remediate any identified deficiencies, and a continuous monitoring program.

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 by completing the Department Risk Management Framework process and receiving an ATO. As part of the ATO, MSIX is required to comply with both the current version of NIST Special Publication 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 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 system implements the Department's Risk Management Framework (RMF) processes and will be included in the Information System Continuous Monitoring (ISCM) program to minimize new threats or vulnerabilities. The continuous monitoring of security and privacy control effectiveness will be facilitated through the Ongoing Security Authorization (OSA) program. The OSA program supports improved risk reporting in accordance with updated NIST guidelines.

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 risks associated with MSIX 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 embarrassment. 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, limiting users to those who are screened, utilizing least privilege principles and encrypting data in transmission. 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 and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.