MSIX User Access Guide and Application

MSIX
Migrant Student Information Exchange

DEPARTMENT OF EDUCATION

MSIX User Access Guide and Application

March 2021

"MSIX IS ONLY AVAILABLE TO AUTHORIZED USERS"

OMB Information Collection Notice 1810-0686 (Expires 7/31/2021)

Table of Contents

MSIX Application Procedure Overview

The MSIX Application Procedure is composed of three processes: Applicant, Verifying Authority, and Final Approving Authority. These processes are discussed in further detail in this guide to provide the steps for obtaining access to MSIX.

Roles in Application Procedure

The following key players participate in the Application Procedure:

- **Applicant** – the potential user requesting access to MSIX
- **Verifying Authority** – the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure who verifies the Applicant's identification, attests to their need for an MSIX account, and confirms the Applicant has the right level of access
- **Final Approving Authority** – the State or Regional User Administrator who gives final approval and creates the Applicant's account

Each of the roles plays a critical part in the application process. The *"User Application for Access to MSIX"* application form is also included at the end of this guide.

Application Procedure

The steps below outline the complete application process:

STEP 1: Applicant Information

- The Applicant completes the Applicant Information and signs the form (see page 15).
- The Applicant forwards the form to a Verifying Authority. This should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure. The Applicant must provide appropriate identification (such as state/district identification badge, passport, driver's license, etc.) to verify their identity and evidence to support completion of a basic cyber security awareness training.

STEP 2: Identification Verification and Attestation

- The Verifying Authority completes his/her own information, reviews the entire application for completeness and accuracy, confirms the Applicant's identification, attests to the Applicant's need of an MSIX account, confirms completion of basic cyber security awareness training and confirms the right level of access.
- Upon completion, the Verifying Authority returns the form to the Applicant.

STEP 3: Forward Form to Approving Authority

- The Applicant locates his/her State/Regional Authority for final approval by going to the MSIX website: https://msix.ed.gov.
- The Applicant clicks on the link labeled "Request An Account" to access the contact information for their state.
- The Applicant forwards the form to the State/Regional Authority for final approval.

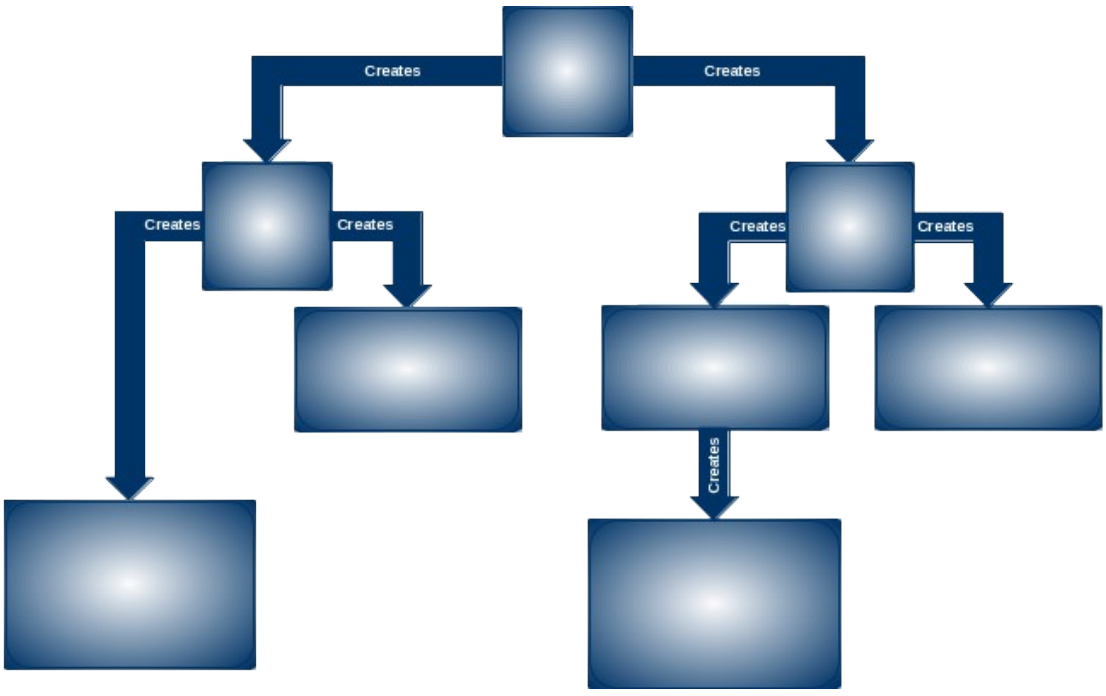
STEP 4: State/Regional Authority Approval

- The State/Regional Authority reviews the Applicant and Verifying Authority portions of the application for completeness, completes his/her own information, signs the form, and files it in his/her local records.
- The State/Regional Authority creates an MSIX account for the Applicant.
- The Applicant receives two emails: one with his/her MSIX User Name and the other with his/her initial Password.

MSIX Account Creation Hierarchy

The figure below displays the account creation hierarchy within MSIX. The OME User Administrator is responsible for creation and maintenance of the State User Administrators.

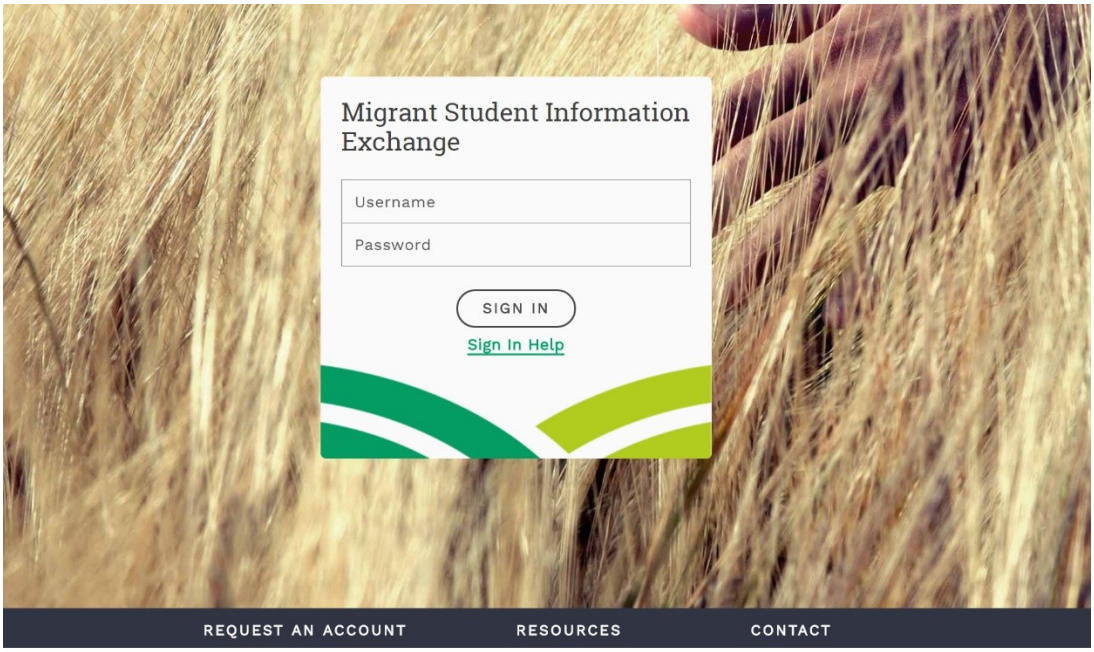
The State User Administrators role differs depending on the use of the MSIX regional structure. If a state does not use the Regional User Administrator role, then the State User Administrator is responsible for the creation and maintenance of all additional roles.

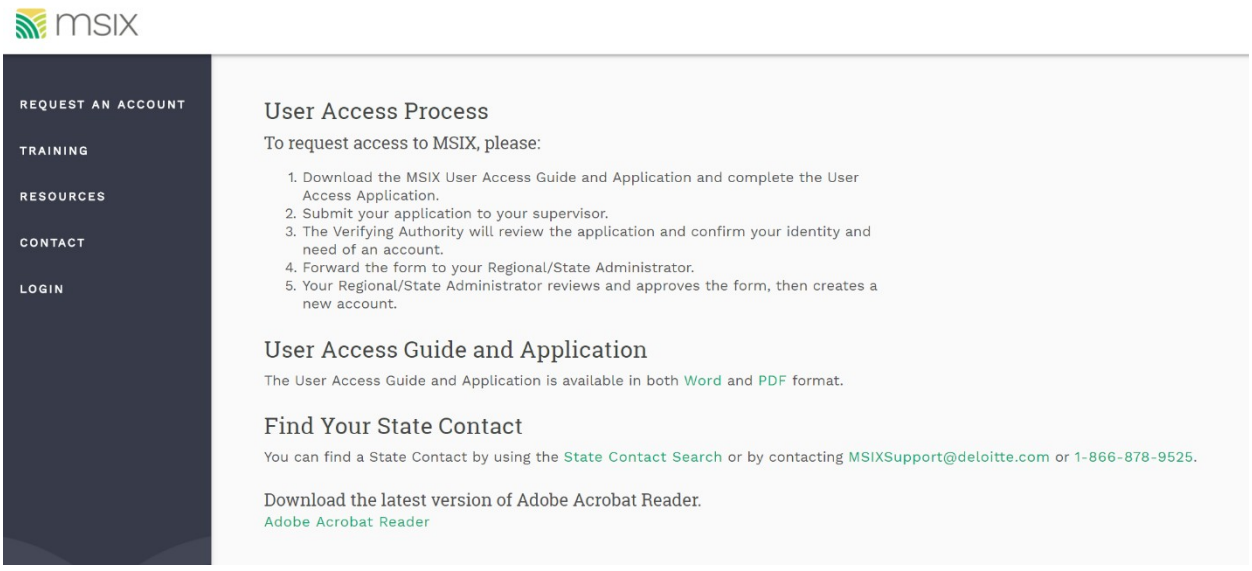


1) Applicant Process

Obtain Application

Applications for access to MSIX can be obtained through the MSIX Sign In screen (https://msix.ed.gov). No login is required and the application form is downloadable from the Request an Account link.





Complete Application

The form is a guideline created to help states with the user registration process. If this form is used, it must be completed in its entirety. The form below displays all of the fields to be completed by the applicant:

Applicant Information

- Complete the applicant information below and sign the form.
- Forward the form to a Verifying Authority. This should be your direct supervisor or an individual that is above the direct supervisor in an official reporting structure. Provide appropriate identification information and proof of cyber security training.

First Name		Last Name			
Cyber Security Training Date	EXAMPLE				
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* - - Ext.		
Region (if applicable)		School District (if applicable)			

Intended Use

Purpose (select one)	☐ Migrant Education Program Participation, School Enrollment, Placement and Secondary Credit Accrual	☐ US Dept of ED, OME Grant Management	☐ **Other:** _____

MSIX Account Information

MSIX Role(s)	☐ Primary User ☐ Secondary User ☐ State Regional Admin	☐ State User Admin ☐ Regional User Admin	☐ State Data Admin ☐ Regional Data Admin ☐ District Data Admin ☐ State Batch Submitter	☐ OME User Admin ☐ Gov. Administrator ☐ MSIX Privacy Act Admin

Job Title

Select all that apply	☐ State MEP Administrator or Staff ☐ Regional/Local MEP Administrator or Staff	☐ MEP Recruiter ☐ School Registrar ☐ Student Liaison/Advocate	☐ Teacher ☐ School Guidance Counselor ☐ Other: Please specify _____	☐ Federal Employee ☐ Federal Contractor

Signature

I certify that this information is accurate and complete to the best of my knowledge. I will only use MSIX in accordance with the MSIX Rules of Behavior.

Signature: _____ Date: _____

Application Information

- **First Name** and **Last Name** – the legal name of the individual requesting access to MSIX

- **Title** – the applicant's job title or description such as Teacher, Guidance Counselor, or Student Registrar
- **Cyber Security Training Date –** the date of most recently completed cyber security training, as required by the MSIX Rules of Behavior
- **Work Address** – the street, city, state and zip code of applicant's workplace
- **Work Email** – the applicant's workplace email address
- **Work Telephone** – the applicant's workplace telephone number

The address, email, and telephone number provided on the application may be used to contact the applicant about MSIX matters.

MSIX Account Information

- **Region** and **District** – the region and district where the applicant works

  Both fields are optional for roles that are not region or district specific; not all states have a regional structure.
- **Intended Use** – the reason for requesting access to MSIX. Requestors from State or Local Education Agencies are expected to select the first option. If selecting "Other," a description of the intended use must be written into the form.
- **MSIX Role** – the desired MSIX user role(s) – see Table 1, *"MSIX User Roles and Responsibilities."*

**Boxes shaded gray on the form are reserved for use by the US Department of Education.*

Signature

- **Signature** – the applicant's certification that the information provided is accurate and complete
- **Date** – the date the applicant signed the application

Once an MSIX user account has been created, the user should update their phone number and password using the **My Account** page in MSIX. Users must contact their State User Administrator to make any other changes to their account, such as changes to name, work address, or email address.

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
State User Category			
Primary	MSIX Primary Users can query student records in all states. This role can also initiate the merge and split process for student records in their state.	▪ Search, display, and print student records ▪ Export a student record to a file for load into a state system ▪ Email notification of a student arrival	▪ MEP Data Entry Staff ▪ Recruiters ▪ Other MEP-Funded Staff

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
		▪ Initiate merge and split of student records ▪ Access to all district-level MSIX Reports	
Secondary	MSIX Secondary Users can query student records in all states.	▪ Search, display, and print student records for students in all states ▪ Email notification of a student arrival ▪ Limited access to MSIX reports	▪ Guidance Counselors ▪ MEP Data Entry Staff ▪ Recruiters ▪ Registrars ▪ Teachers
State Regional Administrator	State Region Administrator establishes and maintains the regional structure and associated districts for states that choose to use regions.	▪ Enable and disable regional structure ▪ Create new regions ▪ Associate districts to regions ▪ Edit regions	▪ State identified
State Data Administrator	State Data Administrators can validate or reject near matches, merges and splits of student records. The role can initiate the merge and split process for student records in their state. This role can also resolve data quality issues and serve as the primary point of contact for escalation issues.	▪ Search, display, and print student records ▪ Export a student record to a file for load into a state system ▪ Email notification of a student arrival ▪ Initiate merge and split of student records ▪ Generate Data and Information Exchange Reports ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ State-level access to MSIX Reports	▪ State MEP Administrators ▪ MEP Data Entry Staff
Regional Data Administrator	Regional Data Administrators can validate or reject near matches, merges and splits of student records. The role can initiate the merge and split process for student records in their state. This role also serves as the secondary point of contact for escalation issues.	▪ Search, display, and print student records ▪ Export a student record to a file for load into a state system ▪ Email notification of a student arrival ▪ Initiate merge and split of student records ▪ Generate Data Reports ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Regional-level access to MSIX reports	▪ State MEP Administrators ▪ MEP Data Entry Staff
District Data Administrator	District Data Administrators can validate or reject near matches, merges and splits of student records. The role can also initiate the merge and split process for student records in their state.	▪ Search, display, and print student records ▪ Export a student record to a file for load into a state system ▪ Email notification of a student arrival ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ District-level access to MSIX reports	▪ State MEP Administrators ▪ MEP Data Entry Staff

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
State User Administrator	State User Administrators establish and manage user accounts for users in their state.	▪ Create user accounts ▪ Assign role(s) ▪ Update user account information ▪ Deactivate user accounts ▪ Reset passwords	▪ State identified
Regional User Administrator	Regional User Administrators establish and manage user accounts for users in their region.	▪ Create user accounts ▪ Assign role(s) ▪ Update user account information ▪ Deactivate user accounts ▪ Reset passwords	▪ State identified
State Batch Submitter	State Batch Submitter upload and transfer student files to MSIX for processing. **Contact MSIX Help Desk for file server access.*	▪ Run data quality reports ▪ Upload and transfer student files to MSIX for processing	▪ State technical team
OME RESERVED ROLES			
OME User Administrator	OME User Administrators establish and manage user accounts for all State User Administrators.	▪ Create / Deactivate user accounts ▪ Assign State User Administrators ▪ Update user account information ▪ Reset passwords	▪ US Dept of ED, OME identified personnel
Government Administrator	OME / Government Administrators can generate summary level standard and ad hoc queries on a State, Regional, or National level.	▪ Generate Reports	▪ US Dept of ED, OME identified personnel
MSIX Privacy Act Admin	Privacy Act Administrators can enter Statements provided by students and parents that formally dispute the data contained in a student's MSIX record. They can also query and view student records from all States.	▪ Search, display, and print student records ▪ Enter dispute Statements into a student's MSIX record	▪ US Dept of ED, OME identified personnel

Table 1 – MSIX User Roles and Responsibilities

Submit to Verifying Authority

The identity of MSIX Applicants should be verified and the type of MSIX access requested must be reviewed. The Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure should perform the identity verification and application review. Further, they attest to the Applicant's need for MSIX and confirm that the correct user roles have been requested. For example, an applicant who is a teacher may submit the application to his or her principal for identity verification and review.

2) Verifying Authority Process

Verify Applicant Identity and User Role

When approving an application, the Verifying Authority should verify the user's identity (e.g., reviewing their State/District issued ID badge, driver's license, passport, etc.). As approver of system access, the Verifying Authority is responsible for verifying the Applicant's identity. The Verifying Authority must review each field of the application for accuracy and completeness. The Verifying Authority will also verify that the Applicant's MSIX role is appropriate for their job. The Verifying Authority is responsible for ensuring that the applicant has completed a basic cyber security awareness training course prior to gaining access. At a minimum, the new user must read and acknowledge the MSIX Rules of Behavior (August 2015 or most current as posted on MSIX).

Complete Verifying Authority Section

Upon successful verification of identity, the Verifying Authority will complete the Identification and Attestation portion on the second page of the application. Upon completion, they should retain a copy of the application for their local records.

Identification Verification and Attestation

- As the Verifying Authority, you should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure.
- Review the entire application for completeness and accuracy.
- Complete the information below, confirm the Applicant's identification, attest to his/her need of an MSIX account, confirm completion of basic cyber security training, and confirm that the Applicant has the right level of access.
- Upon completion, file the form in your local records and return this form to the Applicant.

Verifying Authority First Name	EXAMPLE	Verifying Authority Last Name	
Title			
Work Email		Work Telephone	*XXX-XXX-XXXX* - - Ext.
Organization		Applicant Identity Verification Method	☐ State Driver's License ☐ State / District ID ☐ Passport ☐ Other: _____
Account Effective Date (optional)		Account End Date (optional)	

Signature

I certify that: 1) I have verified the identity of the above applicant; 2) I have determined that he or she has a need for MSIX information; 3) I have confirmed that he or she completed basic cyber security training; and 4) the above-mentioned individual is requesting the appropriate MSIX role(s).

Signature: _____ Date: _____

Identification Verification and Attestation

- **Verifying Authority First Name** and **Verifying Authority Last Name** – the legal name of the Verifying Authority reviewing the application
- **Title** – the official title or position of the Verifying Authority
- **Work Email** – the Verifying Authority's work email address
- **Work Telephone** – the Verifying Authority's workplace telephone number

  The phone number may be used if the Verifying Authority needs to be contacted about MSIX matters.
- **Organization** – the organization or entity that employs the Verifying Authority
- **Applicant Identity Verification Method** – the type of ID or method used to verify the identity of the applicant
- **Account Effective Date** and **Account End Date** – optional fields that can be used to designate a known future start or end date for a user account

  For instance, a future Account End Date may be entered for a seasonal employee that will no longer need access to MSIX after the summer months.

Signature

- **Signature** – the Verifying Authority's certification that the information provided is accurate and complete
- **Date** – the date the applicant signed the application

Applicant Submits Application

Each state may have State User Administrators, Regional User Administrators, or both. The User Administrator will create an account in MSIX for the Applicant requesting access based on information provided in the application. The application should be delivered to the User Administrator's office.

To find the contact information for a State or Regional User Administrator, click on the **Request an Account** link from the MSIX home page (msix.ed.gov), or contact the state's Migrant Education Program office.

3) Approving Authority Process

Review Complete Application

The User Administrator will review the application received to verify that both the Applicant and Verifying Authority sections are complete. If any problems are identified during the review, the User Administrator will contact the Applicant and/or the Verifying Authority that reviewed the application.

Upon successfully completing the review, the User Administrator will create account(s) for the Applicant requesting access to MSIX based upon the information provided in their application.

State/Regional Authority Approval

- Review the Applicant and Verifying Authority portions of the application for completeness.
- Complete the information below, sign, and file the form in your local records.
- Create an MSIX account for the Applicant.

Approving Authority First Name	EXAMPLE	Approving Authority Last Name			
Title		Role	☐ Regional User Administrator ☐ State User Administrator		
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* - - Ext.		

Signature

I certify that this information is accurate and complete to the best of my knowledge and I hereby grant to the above-mentioned individual the MSIX role for which they have applied.

Signature: _____ Date: _____

State/Regional Authority Approval

- **Approving Authority First Name** and **Approving Authority Last Name** – the legal name of the Approving Authority reviewing the application
- **Title** – the official title or position of the Approving Authority
- **Role** – the position of the Approving Authority representing either the regional or state level
- **Work Address** – the street, city, state and zip code of Approving Authority's workplace
- **Work Email** – the Approving Authority's work email address

- **Work Telephone** – the Approving Authority's workplace telephone number

The phone number may be used if the Approving Authority needs to be contacted about MSIX matters.

Signature

- **Signature** – the Approving Authority's certification that the information provided is accurate and complete
- **Date** – the date the applicant signed the application

Next Steps

Once the user account information is successfully entered into MSIX, the User Administrator will be taken to a confirmation page that indicates that the new account was successfully created. MSIX will generate an email notification to the new user, using the email address entered by the User Administrator, to notify them of their new MSIX Username and provide information about accessing MSIX. The User Administrator will be copied on this message as an additional confirmation that the account was created, and the new user notified. MSIX will generate a second separate email message to the new user only, containing the initial password for their new MSIX account. The new MSIX user will be required to reset this password when they first access MSIX.

User Application for Access to MSIX

STEP 1: Applicant Information

- The Applicant completes the Applicant Information and signs the form.
- The Applicant forwards the form to a Verifying Authority. This should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure. The Applicant must provide appropriate identification (such as state/district identification badge, passport, driver's license, etc.) to verify their identity.

STEP 2: Identification Verification and Attestation

- The Verifying Authority completes his/her own information, reviews the entire application for completeness and accuracy, confirms the Applicant's identification, attests to the Applicant's need of an MSIX account, and confirms the right level of access.
- Upon completion, the Verifying Authority returns the form to the Applicant.

STEP 3: Forward Form to Approving Authority

- The Applicant locates his/her State/Regional Authority for final approval by going to the MSIX website: https://msix.ed.gov.
- The Applicant clicks on the link labeled "Request An Account" to access the contact information for their state.
- The Applicant forwards the form to the State/Regional Authority for final approval.

STEP 4: State/Regional Authority Approval

- The State/Regional Authority reviews the Applicant and Verifying Authority portions of the application for completeness, completes his/her own information, signs the form, and files it in his/her local records.
- The State/Regional Authority creates an MSIX account for the Applicant.
- The Applicant receives two emails: one with his/her MSIX User Name and the other with his/her initial Password.

Applicant - Instructions to the Applicant

Applicant Information

- Complete the applicant information below and sign the form.
- Forward the form to a Verifying Authority. This should be your direct supervisor or an individual that is above the direct supervisor in an official reporting structure. Provide appropriate identification information and proof of cyber security training.

First Name		Last Name			
Cyber Security Training Date					
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	- - Ext.		
Region (if applicable)		School District (if applicable)			

Intended Use

Purpose (select one)	☐ Migrant Education Program Participation, School Enrollment, Placement and Secondary Credit Accrual	☐ US Dept of Ed, OME Grant Management	☐ **Other:** _____

MSIX Account Information

MSIX Role(s)	☐ Primary User ☐ Secondary User ☐ State Regional Admin	☐ State User Admin ☐ Regional User Admin	☐ State Data Admin ☐ Regional Data Admin ☐ District Data Admin ☐ State Batch Submitter	☐ OME User Admin ☐ Gov. Administrator ☐ MSIX Privacy Act Admin

Job Title

Select all that apply	☐ State MEP Administrator or Staff ☐ Regional/Local MEP Administrator or Staff	☐ MEP Recruiter ☐ School Registrar ☐ Student Liaison/Advocate	☐ Teacher ☐ School Guidance Counselor ☐ Other: Please specify _____	☐ Federal Employee ☐ Federal Contractor

Signature

I certify that this information is accurate and complete to the best of my knowledge. I will only use MSIX in accordance with the MSIX Rules of Behavior.

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a)

Verifying Authority - Instructions to the Verifying Authority

Identification Verification and Attestation

- As the Verifying Authority, you should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure.
- Review the entire application for completeness and accuracy.
- Complete the information below, confirm the Applicant's identification, attest to his/her need of an MSIX account, confirm completion of basic cyber security training, and confirm that the Applicant has the right level of access.
- Upon completion, file the form in your local records and return this form to the Applicant.

Verifying Authority First Name		Verifying Authority Last Name	
Title			
Work Email		Work Telephone	*XXX-XXX-XXXX* - - Ext.
Organization		Applicant Identity Verification Method	☐ State Driver's License ☐ State / District ID ☐ Passport ☐ Other: _____
Account Effective Date (optional)		Account End Date (optional)	

Signature

I certify that: 1) I have verified the identity of the above applicant; 2) I have determined that he or she has a need for MSIX information; 3) I have confirmed that he or she completed basic cyber security training; and 4) the above-mentioned individual is requesting the appropriate MSIX role(s).

Signature: _____ Date: _____

Final Approving Authority - Instructions to the Final Approving Authority

State/Regional Authority Approval

- Review the Applicant and Verifying Authority portions of the application for completeness.
- Complete the information below, sign, and file the form in your local records.
- Create an MSIX account for the Applicant.

Approving Authority First Name		Approving Authority Last Name			
Title			Role	☐ Regional User Administrator ☐ State User Administrator	
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* - - Ext.		

Signature

I certify that this information is accurate and complete to the best of my knowledge and I hereby grant to the above-mentioned individual the MSIX role for which they have applied.

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a)

Privacy Act Statement

The U. S. Department of Education (Department) will use the information that you provide on the attached MSIX User Application Form to promote secure and appropriate access to the Migrant Student Information Exchange (MSIX) system. The Department owns the MSIX system, including the data stored therein, which has a significant value and is an integral part of the infrastructure that supports the Department's mission, goals and critical operations. It is essential that information in the MSIX system is properly secured and protected against information security related threats and dangers. MSIX has incorporated access controls to protect it against inappropriate or undesired user access. The process of granting and controlling access begins with the completion of the MSIX User Application Form, and the granting of rights and privileges. The MSIX User Application Form serves an integral part of the Department's system to identify and verify authorized users for access to MSIX, assign roles to authorized users of MSIX, tie actions taken within MSIX to a specific user, control access to MSIX and ensure authorized users only have access to MSIX that is needed to perform the actions required by their positions, prevent the inappropriate release of information in MSIX, and document that MSIX users understand the MSIX rules of behavior.

The Department requests the information on the attached Form under the authority provided by section 1308(b)(2) of the Elementary and Secondary Education Act (ESEA), as amended by the Every Student Succeeds Act(P.L. 114-95). Your disclosure of information is voluntary, but if you do not submit the requested information, either on this form or, in a State form, if applicable, that requests that you provide the same information, then you will not be granted access to use the MSIX system.

The Department may disclose information contained in a record in this system of records, under the routine uses listed in this system of records, without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. The Department may make these disclosures on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended (Privacy Act), under a computer matching agreement. Routine uses of records maintained in the MSIX system include:
(1) MEP Services, School Enrollment, Grade or Course Placement, Accrual of High School Credits, Student Record Match Resolution, and Data Correction Disclosure. The Department may disclose a record in this system of records to authorized representatives of SEAs, LEAs, or other MEP LOAs to facilitate one or more of the following for a student: (a) Participation in the MEP, (b) enrollment in school, (c) grade or course placement, (d) credit accrual, (e) unique student match resolution, and (f) data correction by parents, guardians, and migratory children.
(2) Contract Disclosure. If the Department contracts with an entity for the purposes of performing any function that requires disclosure of records in this system to employees of the contractor, the Department may disclose the records to those employees who have received the appropriate level security clearance from the Department. As part of such a contract, the Department will require the contractor to agree to establish and maintain safeguards to

protect the security and confidentiality of the disclosed records.
(3) Research Disclosure. The Department may disclose records from this system to a researcher if an appropriate official of the Department determines that the individual or organization to which the disclosure would be made is qualified to carry out specific research related to functions or purposes of this system of records. The official may disclose information from this system of records to that researcher solely for the purpose of carrying out that research related to the functions or purposes of this system of records. The researcher will be required to agree to establish and maintain safeguards to protect the security and confidentiality of the disclosed records.
(4) Freedom of Information Act (FOIA) or Privacy Act Advice Disclosure. The Department may disclose records to the U.S. Department of Justice (DOJ) or the Office of Management and Budget (OMB) if the Department concludes that disclosure is desirable or necessary to determine whether particular records are required to be disclosed under the FOIA or the Privacy Act.
(5) Disclosure in the Course of Responding to a Breach of Data. The Department may disclose records from this system to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that there has been a breach of the system of records; (b) the Department has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and, (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts in responding to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
(6) Litigation or Alternative Dispute Resolution (ADR) Disclosure.
(a) Introduction. In the event that one of the following parties is involved in litigation or ADR, or has an interest in litigation or ADR, the Department may disclose certain records to the parties described in paragraphs b, c, and d of this routine use under the conditions specified in those paragraphs:
(i) The Department or any of its components.
(ii) Any Department employee in his or her official capacity.
(iii) Any employee of the Department in his or her individual capacity where DOJ has agreed to or has been requested to provide or arrange for representation of the employee.
(iv) Any employee of the Department in his or her individual capacity where the Department has agreed to represent the employee.
(v) The United States where the Department determines that the litigation is likely to affect the Department or any of its components.
(b) Disclosure to DOJ. If the Department determines that disclosure of certain records to DOJ, or attorneys engaged by DOJ, is relevant and necessary to litigation or ADR, and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to DOJ.
(c) Adjudicative Disclosure. If the Department determines that disclosure of certain records to an adjudicative body before which the Department is authorized to appear or to a person or entity designated by the Department or otherwise empowered to resolve or mediate disputes is relevant and necessary to litigation or ADR, and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to the adjudicative body, person, or entity.
(d) Disclosure to Parties, Counsel, Representatives, and Witnesses. If the Department determines that disclosure of certain records to a party, counsel, representative, or witness is relevant and necessary to litigation or ADR, and is compatible with the purpose for which the records were collected, the Department may disclose those records as a routine use to a party, counsel, representative, or witness.
(7) Congressional Member Disclosure. The Department may disclose information from a record of an individual to a member of Congress and his or her staff in response to an inquiry from the member made at the written request of that individual. The member's right to the information is no greater than the right of the individual who requested it.
(8) Disclosure in Assisting another Agency in Responding to a Breach of Data. The Department may disclose records from this system to another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

The System of Record Notice was last published in the federal register on 07/10/2019 (84 FR 32895).

Paperwork Burden Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. The valid OMB control number for this information collection is 1810-0686. Public reporting burden for this collection of information is estimated to average .5 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The obligation to respond to this collection is required to obtain or retain benefit under Title I, Part C of ESSA (P.L. 114-95) Sec. 1304(b)(3) and Sec. 1308 (b)(2). If you have any comments concerning the accuracy of the time estimate, suggestions for improving this individual collection, or if you have comments or concerns regarding the status of your individual form, application or survey, please contact Benjamin Starr, 400 Maryland Avenue, SW, LBJ, Washington, DC, 20202 or Benjamin.starr@ed.gov directly.