

5D

JS



Frank Edelblut
Commissioner

Christine M. Brennan
Deputy Commissioner

STATE OF NEW HAMPSHIRE
DEPARTMENT OF EDUCATION
25 Hall Street
Concord, NH 03301
TEL. (603) 271-3495
FAX (603) 271-1953

November 13, 2023

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

REQUESTED ACTION

For inclusion on the consent calendar. Authorize the Department of Education, Division of Learner Support, to enter into a Memorandum of Understanding with the U.S. Department of Education (USED) for no cost, to support the interconnection of the Migrant Student Information Exchange (MSIX) System owned by the USED and New Hampshire Department of Education's State System (MIS 2000), effective upon Governor and Council approval through December 31, 2026.

EXPLANATION

The New Hampshire Department of Education's (NHED) relationship with MSIX was created to help the state become more effective and efficient in managing the exchange of migrant student educational and health information between and among other states. The MOU was developed to set forth the terms and conditions applicable to the NHED and to govern the relationship and general conditions of data exchange and connectivity between the USED and NHED. The MOU will additionally incorporate the terms of the Interconnection Security Agreement between the USED and NHED. The MOU and security agreement will be effective for a period of three (3) years from the date of execution and will be reviewed and validated via digital signature annually by all parties to ensure that the business needs and details remain.

The MIS 2000 is the system used by the NHED's Migrant Education Program to collect, store, review and verify data on students and families that are part of the State's Migrant Education Program. It is also the system that is used to collect and transmit data to the USED's MSIX system. The collection/transmittal of this data is important to facilitate Migrant Education Program participation, accurate and timely school enrollment, grade and course placement and accrual of course credits.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Frank Edelblut", is written over the "Respectfully submitted," text.

Frank Edelblut
Commissioner of Education

DEPARTMENT OF EDUCATION

Office of Elementary and Secondary Education



Migrant Student Information Exchange (MSIX) Memorandum of Understanding between U.S. Department of Education and

NH Department of Education

**Version 4.3
FIPS 199 Categorization: Low**

Change History

Version	Release Date	Summary of Changes	Affected Page Number(s)	Name
V2	1/15/2016	Update MOU V1 to the latest standard and guidelines	All	Julio Rodriguez
V3	5/19/2017	Update MOU V2 to the latest standard and guidelines	All	Sarah Storms
V4	09/11/2020	Update MOU V3 to the latest standard and guidelines	All	Sarah Storms
V4.1	10/19/2020	Coverted template to PDF format	All	Sarah Storms
V4.2	8/30/2022	Coverted template to PDF format	All	Sarah Storms
V4.3	9/22/2023	Coverted to latest template	All	Sarah Storms

Document Review History

Release Date	Name
September 2017 Version 3.0	Maria Hishikawa, Patricia Meyertholen
September 2020 Version 4.0	Maria Hishikawa, Preeti Choudhary
October 2020 Version 4.1	Preeti Choudhary, Benjamin Starr
August 2022 Version 4.2	Preeti Choudhary, Benjamin Starr
September 2023 Version 4.3	Preeti Choudhary, Benjamin Starr

1.1 Supersession

NH Department of Education

herein referred to as SEA for

the interconnection of the Migrant Student Information Exchange (MSIX) and the State's System,

MIS 2000

herein referred to as State System.

This memorandum between the parties provides access to information stored on information systems owned, operated, and processed at ED as required or allowed by the Federal Information Security Modernization Act (FISMA) of 2014, Office of Management and Budget (OMB) Circular A-130, Appendix I, and National Institute of Standards and Technology (NIST) Special Publication (SP) and Federal Information Processing Standards (FIPS) SP-800-47, SP 800-53 Revision 5, and FIPS-200. It describes the agreement between the parties for the purpose of securing the data on the connected systems. It is the intent of the parties that they will be bound by this MOU once each Designated Approval Authority (DAA) for the connected systems signs it.

This Memorandum of Understanding (MOU) has been developed to establish a management agreement between ED and the SEA when referred to collectively in this agreement, will be described as the “parties.” The systems that are the subject of this MOU are MSIX, owned by ED and the State System used by the SEA. When referred to collectively in this MOU, these systems will be referred to as the “connected systems.”

This MOU sets forth the terms and conditions applicable to the undersigned State educational agency (SEA), the local education agencies (LEAs), and other local operating agencies (LOAs) within the State. Furthermore, this MOU governs the relationship and general conditions of data exchange and connectivity between ED and the SEA, including designated managerial and technical staff, in the absence of a common management authority. The SEA is responsible for requiring LEAs and LOAs under its jurisdiction to use State procedures, including those that govern privacy and security of data, when they forward data to the State information system that will be uploaded into MSIX.

1.4 MSIX

1.4.1 Function

MSIX was created to help States become more effective and efficient in managing the exchange of migrant student educational and health information between and among States by:

- Linking existing State Migrant Exchange Program (MEP) component systems, allowing the free exchange of migrant student information
- Improving the efficiency of the data collection and management process by incorporating the most current Internet-based technologies
- Improving the accuracy and timeliness of information exchanged between States for migrant students
- Increasing information utility by providing information relevant to migrant children and providing users with the appropriate analytic and reporting tools
- Creating accurate, unduplicated counts of the number of migratory children on a Statewide and national basis
- Creating a partnership between ED and the States based on common data standards and data exchange procedures that continually work toward more efficient and effective information sharing methods that improve the educational opportunities for migrant students

1.4.2 Location

MSIX production systems and access points are hosted in Amazon Web Services – East located in Northern Virginia. MSIX disaster recovery system and access points are hosted in Amazon Web Services – West located in Oregon. For security purposes, exact locations are not disclosed by Amazon.

1.4.3 Data Classification

The data being stored, processed, and/or transmitted by MSIX consist of Personally Identifiable Information (PII) regarding migratory children, such as demographics, educational assessments, and course history. This data is classified as Controlled Unclassified Information (CUI). The formal data type as listed in NIST Special Publication (SP) 800-60 is General Government: General Information. MSIX has been determined to have a Security Categorization of low by using the guidance in FIPS 199 and NIST SP 800-60. The MSIX system is configured to the low baseline of controls as defined in NIST SP 800-53 Rev. 4 and also includes the privacy controls.

1.5 State System

1.5.1 Function

Describe the function of the system. This may include the system description that is part of the assessment and authorization of the information system.

MIS2000 is the system used by the New Hampshire Department of Education's Migrant Education Program to collect, store, review and verify data on students and families that are part of the State's Migrant Education Program. It is also the system that is used to collect and transmit data to MSIX.

1.5.2 Location

Give the location address of the functional equipment for both systems (e.g. server room, communications center) and user access points (e.g. building, office number, home).

The central server for New Hampshire's MIS2000 is hosted in Amazon Web Services. Due to security reasons, exact locations are not disclosed by Amazon.

1.5.3 Data Classification

Describe the data to be shared from (State Participating System), including the sensitivity and criticality rankings of the data, which can be found in the system security plan. Include the data types as listed in NIST SP 800-60. In addition, identify any specific security controls required to maintain the protection requirements of the data.

The data being exchanged between MSIX and New Hampshire's MIS2000 is defined in the MSIX Minimum Data Elements and is considered Controlled Unclassified Information (CUI). The data consolidated in MSIX includes Personally Identifiable Information (PII) such as migratory children's names, dates of birth, personal identification numbers assigned by the States and ED, parents' names, school enrollments, school contacts, assessments and other educational and health data necessary to facilitate MEP participation, accurate and timely school enrollment, grade and course placement and accrual of course credits.

1.6 Essential Communications Required Between the Parties to this MOU

Frequent formal communications are essential to ensure the successful management and operation of the connection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in official office memoranda, unless otherwise noted.

The parties agree to designate and provide contact information for technical leads for their respective systems, and to facilitate direct contacts between technical leads to support the management and operation of the connection. To safeguard the confidentiality, integrity, and availability of the data stored, processed, and transmitted on or between the connected systems, the parties agree to provide notice of specific events within the time indicated in this section.

1.6.1 Security Incidents

Technical staff will immediately notify their designated counterparts by telephone or e-mail when a security incident(s) is detected, so the other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. The system owner will receive formal notification within one (1) business day of detecting the incident(s).

Both parties understand and agree that in the event of a security incident affecting the integrity of the data, the interconnection or the interconnected systems, the system administrator of a non-compromised system may cut off access to the affected system with appropriate notice of this decision.

1.6.2 Disasters and Other Contingencies

Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.

1.6.3 Reporting Security Incidents, Disasters and Other Contingencies

The owner of the system experiencing the incident or disaster will send formal written notification to the Designated Approving Authority (DAA) for the other interconnected system within 3 days after detection of the incident(s).

1.6.4 Material Changes to System Configurations

Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the Interconnection Security Agreement (ISA) (described next in this document) within one (1) month of implementation.

1.6.5 New Connections

The initiating party will notify the other party, at least, one (1) month before it connects its IT system with any other IT system, including systems that are owned and operated by third parties.

1.6.6 Personnel Changes

The parties agree to provide notification of the separation or long-term absence (over 60 days) of their respective system owner or technical lead, at least one (1) day before separation or long-term absence. In addition, both parties will provide notification of any changes in point of contact information. Both parties will also provide notification of changes to user profiles, including users who resign or change job responsibilities.

1.7 Interconnection Security Agreement

The technical details of the interconnection will be documented in an ISA. The parties agree to work together to develop the ISA, which must be signed by both parties to continue with the existing interconnection. Proposed changes to either system or the interconnecting medium will be reviewed and evaluated to determine the potential impact on the interconnection. The ISA will be renegotiated before changes are implemented. Signatories to the ISA shall be the DAA for each system.

ED strongly encourages each agency to have and maintain a system security plan that identifies the procedures and controls it will employ to ensure the security of their systems and their interconnection with MSIX. The plan and related documents should be reviewed at least annually, and also in the event of a significant change in their information technology systems or the interconnection with MSIX.

1.7.1 Security

Interconnecting IT systems can expose the participating organizations to risk. If the interconnection is not properly designed and maintained, security failures could compromise the connected system data, or the compromised interconnection could be used as a conduit to attack other systems and data.

Both parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and policies.

MSIX is subject to inspection, security reviews, or modification of procedures or specifications for interconnectivity, contingency planning, and changes in the system. MSIX is also subject to periodic audits to detect and track unusual or suspicious activities across interconnections that might indicate intrusion or internal misuse. When one of these events occurs, the SEA agrees to provide ED, MSIX Team, and ED's contractor with access to its technological specifications, equipment, and records, including security artifacts and audit logs.

1.7.2 Cost Considerations

Each party agrees to pay its share of the costs of the interconnecting mechanism and/or media. Modifications to either system that are necessary to support the interconnection are the responsibility of the respective system owners' organization.

1.8 DAA Resolution and Consent to Monitoring

In the event of suspected fraud, abuse, or security infraction, the DAA for either connected system may conduct an analysis and investigation. After the initial phases of the incident response plan have been executed (specifically, the response, containment, and subsequent triage of the event), the DAA or point of contact should be notified and provided with the information that is known at that point in time. Within five days of receipt of a written request for information, the DAA for the system that is the subject of the investigation shall provide all relevant documentation and other evidence or information necessary to support the investigation.

1.9 Duration of the MOU

The MOU may be terminated upon thirty days written notice by either party, where the connection is not required by law. A shorter termination period is allowed in the event of a security incident or disaster that requires immediate action. This MOU will be effective for a period of three (3) years from the date of execution and will be reviewed and validated via digital signature annually by all parties to ensure that the business needs and details remain current.

1.10 Security Considerations of the MOU

The undersigned SEA agrees to:

- Ensure that only authorized and cleared personnel of its agency, and of the LEAs and LOAs in the State who will connect with MSIX, will be permitted access to MSIX, and that they will adhere to the ED's Password Policy and MSIX Rules of Behavior.
- Notify the State User Administrator of any changes to the identities of authorized and cleared personnel, such as in the event of a change in position or need, for cause, to investigate and suspend or terminate access.
- Have the appropriate safeguards in place to protect against, as well as to respond to, any breaches of the system.
- Limit the use of data, information, and records within MSIX for the purposes of facilitating a migratory child's: (i) participation in the MEP, (ii) enrollment in school, (iii) grade or course placement, (iv) credit accrual, and (v) unique student match resolution.
- Access MSIX only through a secure Internet connection, and be responsible for maintaining and operating its own equipment and information and records systems.
- Be responsible for, and assume any risk associated with, compromises of MSIX associated with the interconnection of the State information system with MSIX.
- Input information into MSIX in accordance to the MSIX Data Exchange Interface Requirements Specification document.

- Allow authorized users access through the creation of MSIX user accounts in accordance with the MSIX User Access Guide and Application.
- Submit only information that is requested by MSIX; particularly, SEAs should not submit Social Security Numbers to MSIX in any form.

Nothing in this MOU shall be construed to waive any right the SEA or State has in law to a defense of sovereign immunity in any action that may arise because of operation of MSIX, or otherwise to create any right or benefit, substantive or procedural, enforceable at law or in equity by third parties against the SEA, State, or the ED or any of their officers, employees, or agents.

Signatory Authority

I agree in full to the terms of this Memorandum of Understanding.

**Department of Education
MSIX Information System Owner**

Frank Edelblut
Digitally signed by Frank
Edelblut
Date: 2023.12.21 09:36:44
-05'00'

State Education Agency: NH Department of Education

State System: MIS 2000

Designated Approving Authority (DAA)

FOR OFFICIAL USE ONLY

DEPARTMENT OF EDUCATION

Office of Elementary and Secondary Education



Migrant Student Information Exchange (MSIX) Interconnection Security Agreement between U.S. Department of Education and

NH Department of Education

Version 4.4

FIPS 199 Categorization: Low

Approval Date:

This document contains Department of Education Sensitive Material and is exempted from release under the Freedom of Information Act by Exemption b(2). US Department of Education Staff reviewing this document must hold a minimum of Public Trust Level 6C clearance.

FOR OFFICIAL USE ONLY

Document Change History

Date	Filename / Version #	Author	Revision Description
1/15/2016	MSIX ISA Template 2016/ V2	Julio Rodriguez	Update ISA V1 to the latest standard and guidelines
2/23/2016	MSIX ISA Template 2016/ V3	Julio Rodriguez	Update ISA V2 to address level of detail for Connection Safeguards
5/17/2017	MSIX ISA Template 2017/ V4	Sarah Storms	Update ISA V3 to latest template and updated Section 3.1.1
7/14/2017	MSIX ISA Template 2017/ V4	Letetia J Kimpson	Updates from feedback from IV&V/ED
8/01/2017	MSIX ISA Template 2017/ V4	Letetia J Kimpson	Updated architecture diagram based on Go Live requirements
08/15/2017	MSIX ISA Template 2017/ V4	J. Hawkins	Update to include feedback from ED review, added section 2.0
09/08/2020	MSIX ISA Template 2020 / V4	S. Storms	Updated MSIX Topology Drawing and MSIX ATO Date
10/14/2020	MSIX ISA Template 2020 / V4	S. Storms	Converted template to PDF format
7/19/2023	MSIX ISA Template 2023 / V4	S. Storms	Updated to latest Dept of ED template

Document Review History

Date	Version #	Reviewers
July 2017	4.0	Patricia Meyertholen Maria Hishikawa
September 2017	4.1	Patricia Meyertholen Maria Hishikawa
September 2020	4.2	Preeti Choudhary Maria Hishikawa
October 2020	4.3	Preeti Choudhary Benjamin Starr
July 2023	4.4	Preeti Choudhary Benjamin Starr

TABLE OF CONTENTS

Document Change History	ii
Document Review History	iii
1 SYSTEM BACKGROUND	1
1.1 Purpose	1
1.2 Scope	1
2 INTERCONNECTION STATEMENT OF REQUIREMENTS	2
2.1 Services Offered	2
2.2 Data Sensitivity	2
2.3 User Community	2
2.4 Trusted Behavior Expectations	3
2.5 Formal Security Policy	3
3 INTERCONNECTION SECURITY AGREEMENT BETWEEN ED'S MSIX AND SEA'S SYSTEM	4
3.1 Description of Connections	4
3.1.1 Location	4
3.1.2 Connection Type	4
3.1.3 Point of Demarcation	6
3.1.4 Accreditation Boundary	6
3.1.5 Data Classification	6
3.1.6 System Accreditation	6
3.2 Topology Drawing	6
3.3 Duration of The Interconnection Security Agreement	8
3.4 Security Considerations of the ISA	8
Appendix A: Acronyms	10
Appendix B: Connection Safeguards	11

1 SYSTEM BACKGROUND

1.1 Purpose

The purpose of this document is to provide guidance for planning, establishing, and maintaining the interconnection between ED's MSIX system and Participating State Education Agency,

NH Department of Education

herein referred

to as SEA and the SEA's system, MIS 2000

herein referred to as State System.

1.2 Scope

This ISA covers only the interconnections between the SEA's State System and MSIX to exchange data. This ISA does not include additional systems.

2 INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between ED and the SEA are for the express purpose of exchanging data between MSIX, owned by ED, and the State System used by the SEA. The Elementary and Secondary Education Act of 1965 (ESEA), as amended by the Every Student Succeeds Act (ESSA), mandated that ED ensure that all students have equal access to education and that ED promote educational excellence throughout the nation. The Office of Migrant Education (OME), part of ED's Office of Elementary and Secondary Education (OESE), is responsible for administering the Migrant Education Program (MEP). The MEP supports SEAs by providing funding to help SEAs establish or improve educational programs for migrant students.

Section 1308(b) of the ESEA requires the OME to assist States in developing effective methods for electronically exchanging student records among States; and to determine and accurately account for the number of migratory children in each State. OME established the MSIX project to satisfy these requirements and support their goals for the MEP through MSIX.

2.1 Services Offered

No user services are offered. This connection only exchanges migrant student data between ED's MSIX and the SEA's State System via a dedicated Secure File Transfer Protocol (SFTP) connection. The service offered is to ensure the linkage of State migrant student records systems into a national platform for the electronic exchange of migrant student educational and health data. After processing and consolidation, the data can be accessed by authorized users through the MSIX secure web-based interface for the purposes of facilitating a student's: (i) participation in the MEP, (ii) enrollment in school, (iii) grade or course placement, (iv) credit accrual, and (v) unique student match resolution.

2.2 Data Sensitivity

The data being exchanged between MSIX and the State system is defined in the MSIX Minimum Data Elements, and is considered Controlled Unclassified Information (CUI). The data consolidated in MSIX includes Personally Identifiable Information (PII) such as migratory children's names, dates of birth, personal identification numbers assigned by the States and ED, parents' names, school enrollments, school contacts, assessments, and other educational and health data indicators necessary to facilitate MEP participation, accurate and timely school enrollment, grade and course placement, and accrual of course credits.

2.3 User Community

All ED users with access to the data received from the SEA hold a valid and current ED background investigation. All SEA users with access to the data in MSIX are authorized and cleared by the SEA. The MSIX end user community accesses the information consolidated in MSIX via a secure web-based interface. MSIX end users do not have access to the back-end infrastructure. The State's authorized technical and data personnel maintain the interconnection with MSIX on the originating system side. States must contact the MSIX Technical team to receive account information for the MSIX File Transfer Protocol (FTP) Server to submit files.

The MSIX System Security Plan includes detailed descriptions for each MSIX user role and access permissions available to users with approval.

2.4 Trusted Behavior Expectations

ED's MSIX system and users are expected to protect the SEA's State System, and SEA's State System and users are expected to protect ED's MSIX system, in accordance with Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710). All MSIX users are required to comply with the MSIX Rules of Behavior.

2.5 Formal Security Policy

Policy documents that govern the protection of the data exchange through this interconnection are below:

- Federal Information Security Modernization Act of 2014 (FISMA)
- OCIO 03-112 Cybersecurity Policy
- Privacy Act of 1974
- Unauthorized Access Act (18 U.S. Code 2701)
- Office of Management and Budget (OMB) Circular
 - A-130 Managing Information as a Strategic Resource
 - Appendix I: Responsibilities for Protecting and Managing Federal Information Resources
- National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS)
 - SP 800-47 Security Guide for Interconnecting Information Technology Systems
 - SP 800-53 Revision 5 Security and Privacy Controls for Federal Information Systems And Organizations
 - FIPS 200 Minimum Security Requirements for Federal Information and Information

3 INTERCONNECTION SECURITY AGREEMENT BETWEEN ED'S MSIX AND SEA'S SYSTEM

3.1 Description of Connections

3.1.1 Location

- **MSIX:** MSIX production systems and access points are hosted in Amazon Web Services – US East Region. MSIX disaster recovery system and access points are hosted in Amazon Web Services – US West Region. Due to security reasons, exact locations are not disclosed by Amazon.
- **State System:** *Give the location address of the functional equipment for the State System (e.g., server room, communications center) and user access points (e.g., building, office number, home).*

MIS2000 production systems and access points are hosted in Amazon Web Services – US East Region. Due to security reasons, exact locations are not disclosed by Amazon.

3.1.2 Connection Type

The connection type used in this interconnection is a major application to a major application. The external data transport services between MSIX and the system use SFTP.

The data that will traverse the connection include Personally Identifiable Information (PII) regarding migratory children, such as demographics, educational assessments, and course history. SEAs will upload this data to MSIX in the format of

Extensible Markup Language (XML).

Each SEA is provided with a dedicated location for its files on the FTP server, as well as a unique login credential (i.e., User ID). States are required to create a public/private key pair and submit the public key to the MSIX Technical Team for authentication.

MSIX uses a file-based interface system, known as the State Systems Interface (SSI). Each interface in this system is used to receive and send MSIX student files from and to the system.

The following table provides details of these 5 interfaces:

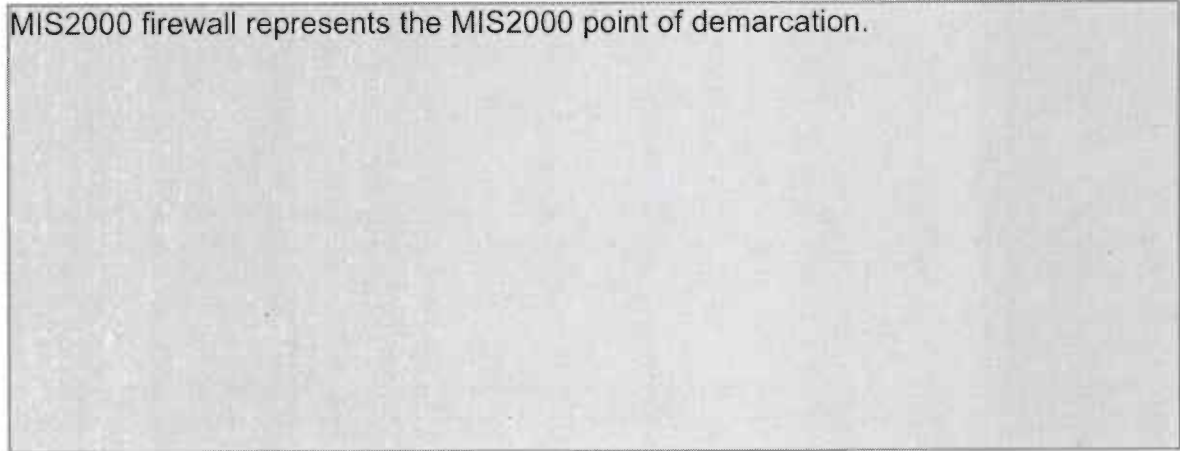
Interface File Type	Inbound/Outbound	Description
State Systems Inbound Interface (SSII)	Inbound	MSIX will use a file-based interface, known as the State Systems Inbound Interface (SSII), as its primary method for receiving data from each State's migrant education system. The SSII allows States to submit migrant student data to MSIX using delimited flat or Extensible Markup Language (XML) file formats that support the MDE.
State Systems Outbound Response Interface (SSORI)	Outbound	MSIX will use a file-based interface, known as the State Systems Outbound Response Interface (SSORI), as its primary method for sending automated response files to each State's migrant education system using delimited flat or XML file formats that support the MDE. This file is generated to provide outcome of processing SSII file.
State Systems Outbound Response Error Interface (SSOREI)	Outbound	MSIX will use a file-based interface, known as the State Systems Outbound Response Error Interface (SSOREI), as the method for to provide processing and error details of each student record submitted in the SSII file by the State System.
State Systems Outbound OnDemand Interface (SSOOI)	Outbound	MSIX will use a file-based interface, known as the State Systems Outbound OnDemand Interface (SSOOI), as its primary method for sending on-demand requests for a student's consolidated file to each State's migrant education system using delimited flat or XML file formats that support the MDE.
State Systems Outbound Merge Split Interface (SSOMSI)	Outbound	MSIX will use a file-based interface, known as the State Systems Outbound Merge Split Interface (SSOMSI), as its primary method

		for sending files to States when a student in their State is involved in a merge or a split within MSIX.
--	--	--

3.1.3 Point of Demarcation

- **MSIX:** The MSIX firewall represents the point of demarcation.
- **State System:** *List the logical components at which control over and protection of the data becomes responsibility of the other system (e.g., MIS2000 firewall represents the MIS2000 point of demarcation)*

MIS2000 firewall represents the MIS2000 point of demarcation.



3.1.4 Accreditation Boundary

- **MSIX:** The MSIX firewall represents the MSIX accreditation boundary.
- **State System:** System accreditation requirements under FISMA do not apply to State owned and operated systems.

3.1.5 Data Classification

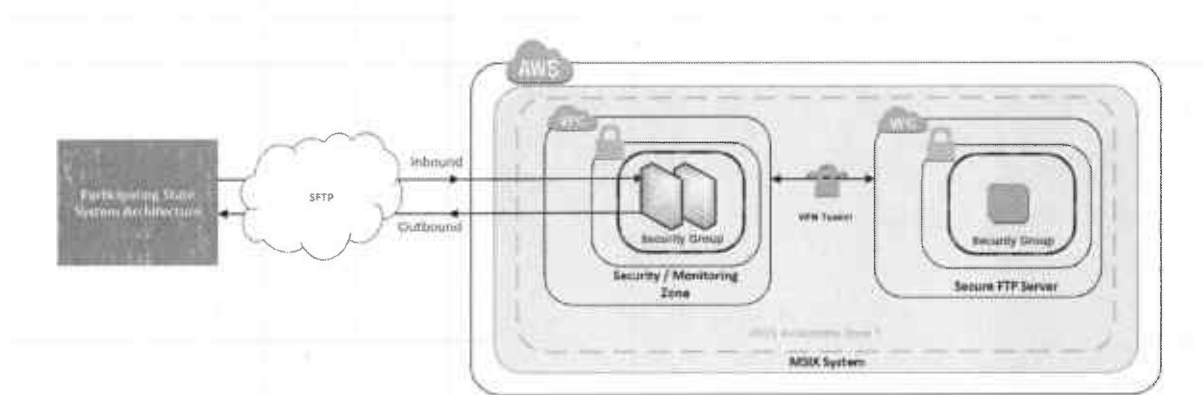
The data exchanged between MSIX and the State system include migratory children's demographic, assessment, course history, and immunization data. This data is classified as Controlled Unclassified Information (CUI) and has a Low Security Categorization.

3.1.6 System Accreditation

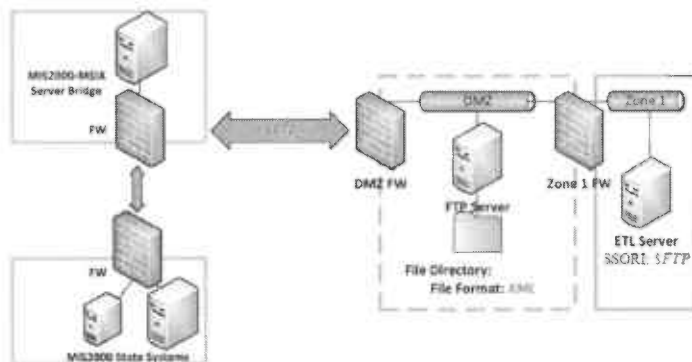
- **MSIX:** The MSIX firewall represents the MSIX accreditation boundary.
- **State System:** System accreditation requirements under FISMA do not apply to State owned and operated systems.

3.2 Topology Drawing

- **MSIX:**



- State System:** Insert a logic drawing showing systems and boundaries, which emphasizes where data of one system is placed in the other system or transported between access points.



3.3 Duration of The Interconnection Security Agreement

This ISA shall terminate in the event that contracts with ED's MSIX system and the SEA's State System terminate, or the requirement for a direct communication link no longer exists. This ISA will be effective for a period not to exceed three years from the date of execution; however, it will be reviewed annually to ensure that the technical details remain current. This ISA must not exceed the duration of the Memorandum of Understanding it supports.

3.4 Security Considerations of the ISA

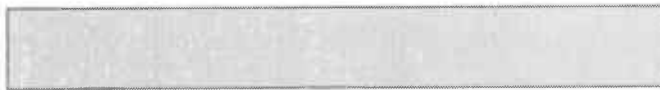
ED and the SEA agree to protect the ISA from unauthorized disclosure and modification. The ISA will only be disclosed to cleared authorized personnel through the use of secure mechanisms (e.g. encrypted email, secure fax). Digital copies must be encrypted and nondigital copies must be secured appropriately.

Signatures

MSIX Officials

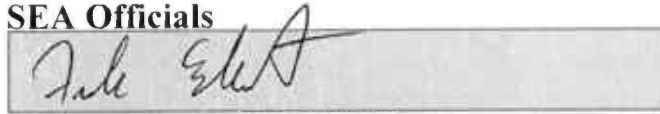


MSIX Information System Owner
U.S. Department of Education



MSIX Information System Security Officer
U.S. Department of Education

SEA Officials



Name: Frank Edelblut, Commissioner of Education

Designated Approving Authority (DAA)

Participating SEA: NH Department of Education

Victor R. Oliver Digitally signed by Victor R. Oliver
Date: 2023.10.19 08:51:33 -05'00'

Name: Victor R. Oliver

Technical Lead

Participating SEA: NH Department of Education

Appendix A: Acronyms

ACRONYM	ACRONYM NAME
ATO	Authority to Operate
CM	Configuration Management
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
ED	United States Department of Education
ESEA	Elementary and Secondary Education Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISA	Interconnection Security Agreement
MEP	Migrant Education Program
MOU	Memorandum of Understanding
MSIX	Migrant Student Information Exchange
NIST	National Institute of Standards and Technology
OESE	Office of Elementary and Secondary Education
OMB	Office of Management and Budget
OME	Office of Migrant Education
PII	Personally Identifiable Information
SFTP	Secure File Transfer Protocol
SP	Special Publication
SSI	State Systems Interface
SSII	State Systems Inbound Interface
SSOMSI	State Systems Outbound Merge Split Interface
SSOOI	State Systems Outbound OnDemand Interface
SSOREI	State Systems Outbound Response Error Interface
SSORI	State Systems Outbound Response Interface
XML	Extensible Markup Language

Appendix B: Connection Safeguards

Both parties agree that the safeguards implemented on their systems are in place and operating effectively as described in their respective system's system security documentation. The technical safeguards listed below are implemented prior to, and as a condition of, establishing and maintaining a secure connection between and within the domain of the sites. The controls listed here are a subset of the technical controls required by Federal Information Processing Standards (FIPS) 200 and are augmented to meet the needs of the parties.

Technical Security Controls Status for Connection		
Current status of the control as Planned (P), Implemented (I), or Not Applicable (N/A)		
	MSIX	
	FIPS-199 Security Category (Low)	Brief Description
Control		
Access Control (AC)		
AC-1	I	ACCESS CONTROL POLICY AND PROCEDURES
AC-2	I	ACCOUNT MANAGEMENT
AC-3	I	ACCESS ENFORCEMENT
AC-4	N/A	
AC-5	N/A	
AC-6	N/A	
AC-7	I	UNSUCCESSFUL LOGON ATTEMPTS
AC-8	I	SYSTEM USE NOTIFICATION
AC-9	N/A	
AC-10	N/A	
AC-11	N/A	
AC-12	N/A	
AC-13	N/A	
AC-14	I	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
AC-15	N/A	
AC-16	N/A	
AC-17	I	REMOTE ACCESS
AC-18	N/A	
AC-19	N/A	
AC-20	I	USE OF EXTERNAL INFORMATION SYSTEM
Audit and Accountability (AU)		
AU-1	I	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU-2	I	AUDIT EVENTS
AU-3	I	CONTENT OF AUDIT RECORDS
AU-4	I	AUDIT STORAGE CAPACITY
AU-5	I	RESPONSE TO AUDIT PROCESSING

Technical Security Controls Status for Connection		
Current status of the control as Planned (P), Implemented (I), or Not Applicable (N/A)		
	MSIX	
	FIPS-199 Security Category (Low)	Brief Description
		FAILURES
AU-6	I	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-7	N/A	
AU-8	I	TIME STAMPS
AU-9	I	PROTECTION OF AUDIT INFORMATION
AU-10	N/A	
AU-11	I	AUDIT RECORD RETENTION
Identification and Authentication (IA)		
IA-1	I	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
IA-2	I	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-3	N/A	
IA-4	I	IDENTIFIER MANAGEMENT
IA-5	I	AUTHENTICATOR MANAGEMENT
IA-6	I	AUTHENTICATOR FEEDBACK
IA-7	I	CRYPTOGRAPHIC MODULE AUTHENTICATION
System & Communication Protections (SC)		
SC-1	I	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC-2	N/A	
SC-3	N/A	
SC-4	N/A	
SC-5	I	DENIAL OF SERVICE PROTECTION
SC-6	N/A	
SC-7	I	BOUNDARY PROTECTION
SC-8	N/A	
SC-9	N/A	
SC-10	N/A	
SC-11	N/A	
SC-12	I	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-13	I	CRYPTOGRAPHIC PROTECTION
SC-14	N/A	
SC-15	N/A	
SC-16	N/A	
SC-17	N/A	
SC-18	N/A	
SC-19	N/A	
System and Information Integrity (SI)		
SI-1	I	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SI-2	I	FLAW REMEDIATION

Technical Security Controls Status for Connection		
Current status of the control as Planned (P), Implemented (I), or Not Applicable (N/A)		
	MSIX	
	FIPS-199 Security Category (Low)	Brief Description
SI-3	I	MALICIOUS CODE PROTECTION
SI-4	I	INFORMATION SYSTEM MONITORING
SI-5	I	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
SI-6	N/A	
SI-7	N/A	
SI-8	N/A	
SI-9	N/A	
SI-10	N/A	
SI-11	N/A	
SI-12	I	INFORMATION HANDLING AND RETENTION