Privacy Impact Assessment (PIA)

for the

MSAP

May 7, 2021

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

Contact Point

Contact Person/Title: Brandon Dent
Contact Email: brandon.dent@ed.gov

System Owner

Name/Title: Metasebia Belachew
Principal Office: OESE

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Magnet Schools Assistance Program Technical Assistance Center (MSAP TA Center) website is a non-mission critical site that assists the MSAP TA Center contractor, Leed Management Consulting, Inc., in fulfilling its contract with the Magnet Schools Assistance Program (MSAP) in providing technical assistance and performance monitoring activities for MSAP grantees. The external-facing part of the site provides the public with information about the MSAP program and grantees, as well as magnet schools generally. The internal, password-protected part of the site collects Annual Performance Report information to generate regular Government Performance and Results Act (GPRA) reports. In order to obtain the required GPRA information, the system collects and maintains grantee users' office email address and user ID.

Leed Management Consulting, Inc., is responsible for the development, coordination of program business components, system maintenance, and continuous implementation of the MSAP TA Center website according to customer requirements and security standards set forth by the U.S. Department of Education.

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

Information collected is used to provide login credentials to access the system, which is a website that is used to disseminate MSAP guidance information and for sharing best practices and success stories. The grantee information is collected to provide access to the system and facilitate communication between grantees and MSAP team. The organization (State Educational Agencies [SEA] and Local Educational Agencies [LEA]) information submitted by grantees is required as part of the reporting requirements. The grantee information that is posted publicly on the website is the

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

organizational information of the grantee for enabling the community to contact the grantees.

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?

New PIA

There are no changes to the system, but it was determined by Department officials during a recent review of the system that the system maintains PII. As a result, the PTA needed to be revised, a PIA needed to be drafted, and privacy controls needed to be selected and implemented.

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.

MSAP collects data as defined in 34 CFR 280: https://www.gpo.gov/fdsys/pkg/CFR-2016-title34-vol1/xml/CFR-2016-title34-vol1-part280.xml" https://www.gpo.gov/fdsys/pkg/CFR-2016-title34-vol1/xml/CFR-2016-title34-vol1-part280.xml . The statutory authority is 20 U.S.C. 7231-7231j,

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

No

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Click here to enter text.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☐ N/A

The information is not retrieved by an identifier.

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

ED 254A.2/GRS 1.2/ item 020.
TEMPORARY: Destroy 10 years after final action is taken on file, but longer retention is authorized if required for business use.

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

Yes

3. Characterization and Use of Information

[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

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.

Grantee

- Office address
- Office email address
- Office phone number
- Password, for the purpose of proving access.
- Username, which is the email address of the grantee, for the purpose of proving access.

Name of Federal Program Officer – Department of Education Employees

- Office address
- Office email address
- Office phone number

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

Yes

The system collects only name and contact information to establish user accounts for the website and provide the users the ability to contact the grantees by fellow grantees. This is the minimum PII necessary to establish the accounts. Organization phone number is collected to provide contact information for resolving technical assistance requests.

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

Information is provided by grantees who are LEAs and SEAs points of contacts to the Department of Education Program Officer as part of the grant management process, which is provided to the system administrator to load on the site.

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 data are collected by the Department of Education Program Officer during the grantee awarding process through grant application forms and then then loaded by the sysadmin to the website. Information that is collected and disseminated is stored in a

SQL Server database backend. The MSAP system is maintained by the MSAP contractor.

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 PII information on the website is confirmed by the Federal Program Officer annually as part of the grant management process. When the personnel changes at the grantee organization, the change is confirmed by the Federal Program Officer by email

The system sends a verification email to the email address supplied to verify the contact details through a confirmation email. The user is responsible for making updates and ensuring the data on the website are correct.

Use

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

The information collected is used to create user login credentials to allow the grantees to receive technical assistance, submit performance reporting and receive information disseminated by the center through the website.

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

3.8. 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.

There is a Privacy Policy listed on all pages on the page HYPERLINK "https://msapcenter.ed.gov/privacypolicy.aspx" https://msapcenter.ed.gov/privacypolicy.aspx

PRIVACY POLICY

Some of our pages feature forms that let you voluntarily submit personal information, such as your name or e-mail address. For example, this occurs when you submit a Request for Technical Assistance. In all cases, submitted information is used only for the purposes described on the form and is not made available to any third party.

This website contains links to other sites. Please be aware that the Magnet Schools Assistance Program Technical Assistance Center (MSAP Center) is not responsible for the privacy practices of these sites. Also, when users leave our site, we encourage them to read the privacy statements of every website that potentially collects personally identifiable information.

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.

https://msapcenter.ed.gov/privacypolicy.aspx

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?

Grantees are required by Title IV Part D to submit the PO information to ED program office. The users are required to consent to the policy before using the system.

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

Information is never shared with any external personnel or agency.

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

☑ N/A

Click here to enter text.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

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

☑ N/A

Click here to select.

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

☑ N/A

Click here to enter text.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

[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.

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

Grantees have access to their profiles by logging in. Grantees can view and verify the data. Grantee users must contact the MSAP Center Technical Assistance Team to make changes to the information they provided. The technical support teams verify the information before correcting the information.

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

Grantee users must contact the MSAP Center Technical Assistance Team to make changes to the information they provided. The technical support teams verify the information before correcting the information.

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

There is a user guide which provides instructions on how to correct information in the grantee's profile. Users are given training when they are added on how to correct their information.

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?

MSAP access is only available to authorized users. User access is managed by the MSAP office. MSAP only supports communication using the latest secured Transport Layer Security protocols. The system does not collect data from other systems or share data with other systems. All personnel working with MSAP must agree to established rules of behavior. Personnel in system administration and support roles must complete personnel background screening and complete additional training including role-based, incident response, and disaster recovery training.

Physical security is inherited and maintained by the Amazon Web Services GovCloud. MSAP technical and administrative controls comply with the Federal Information Security Modernization Act requirements and with National Institute of Standards and Technology (NIST) standards.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

System undergoes monthly scans and annual security assessment reviews, and the system is continuously monitored using endpoint protection tools.

8. Auditing and Accountability`

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The MSAP system owner ensures that the information is used following stated practices in this PIA through several methods. One method is completing the Department Risk Management Framework process and receiving an authorization to operate. Under this process, a variety of controls are assessed by an independent assessor to ensure the MSAP application and the data residing within are appropriately secured and protected. One-third of all NIST security controls are tested each year, and the entire system's security is re-evaluated regularly. The PIA is reviewed and updated on an as-needed basis and, at a minimum, biennially. These methods ensure that the information is used within the stated practices outlined in this PIA.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary and by not collecting any sensitive PII.

Role-based access controls are implemented to ensure access to data is restricted to authorized users only. Access to monitoring and auditing related documents is limited to Department employees with appropriately approved access authorization. User ID is displayed in the reporting page and is visible to the user who is logged in, but no other PII will be posted to the MSAP Public Portal for any reason. Since users voluntarily decide what to share in report submissions, there is a possibility that PII could be exchanged through these reports.

The privacy risk associated with the system is minimal, as the system only stores grantee names, office email addresses, office phone numbers, user IDs, and passwords. The

system only collects and maintains the minimal information needed for maintaining the login credentials and managing the grants.