Privacy Impact Assessment (PIA)
for the

Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings (IDEA ACDM)
February 18, 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: Stephanie Jackson / Project Director American Institutes for Research
Contact Email: sjackson@air.org

System Owner

Name/Title: Renee Bradley
Principal Office: Office of Special Educational and Rehabilitative Services (OSERS)

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 Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings (IDEA ACDM) system consolidates Office of Special Education Programs (OSEP) Communications and OSEP National Meetings websites. Four of the five websites listed here are Drupal content management systems with containerized web tiers connected to a fully managed MySQL database. Authentication and authorization to manage content is handled by Drupal. There is no other back-end data collection, maintenance, or processing for the Drupal sites. The public site is a read-only site with no authentication. Data is obtained from the client and deployed to the database once every quarter.

These websites are the primary source for teachers, leaders, and families to access information and evidence-based products to improve services for children with disabilities. The consolidated IDEA ACDM is composed of:

- https://osepideasthatwork.org/
- https://publicddb.osepideasthatwork.org/
- https://ccrs.osepideasthatwork.org/
- https://osepideasthatwork.org/osep-meeting
- https://engage.osepideasthatwork.org/

The IDEA ACDM system supports the Office of Special Education Programs (OSEP) Research to Practice Division in accomplishing tasks related to the implementation of the Part D national programs of the Individuals with Disabilities Education Act (IDEA). These tasks include conducting annual meetings and performing program analysis to determine promising practices to communicate to educators and families. OSEP is dedicated to improving results for infants, toddlers, children, and youth with disabilities ages birth through 21. These websites are critical to addressing that mission. OSEP, directly and through its partners and grantees, develops a wide range of products, publications, and resources to assist states, local district personnel, and families to improve results for students with disabilities.

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

[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

used, maintained or shared.

Three of the websites in this consolidation collect personally identifiable information (PII). The National Meetings website (https://osepideasthatwork.org/osep-meeting) provides the public with information about upcoming Office of Special Educational and Rehabilitative Services (OSERS)/OSEP conferences and virtual symposia and collects PII on conference attendees through an online registration portal. These conferences include the National OSEP Project Directors' Conference (a requirement for all grantee Project Directors), the OSEP Leadership Conference, held annually, and other meeting events requiring registration. PII is collected to allow individuals to register for these events, for communication regarding the event, and to make nametags. PII includes the registrant's name, professional affiliation, contact email, and OSEP grant number. Registrants may also indicate that they need an accommodation during the event, such as a sign-language interpreter, so that the accommodation can be provided.

The OSEP Collaboration Spaces website (https://collab.osepideasthatwork.org/) and the Engage OSEP (https://engage.osepideasthatwork.org/) are virtual collaboration spaces designed to bring a variety of stakeholders together to share information and problem solve to improve outcomes for children with disabilities. They are virtual locations where individual grantees can share and exchange thoughts and ideas, share resources, and collaborate on the creation of new knowledge. PII collected for this website includes names and professional email addresses to allow for the registration of members to the spaces and workgroup communication. Users may choose to post additional PII however that is not promoted. The OSEP Collaboration Spaces is being phased out, planned for May 2021, as the Engage OSEP site is fully launched with 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?

Updated PIA

This PIA is being updated pursuant to the Department's policy requiring bi-annual review of PIAs.

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

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.

The authority to collect and use this data is derived from the Individuals with Disabilities Education Act (IDEA), 20 USC Ch. 33, Part D. IDEA, Part D addresses "National Activities to Improve Education of Children with Disabilities." It includes provisions related to discretionary grants to support state personnel development, technical assistance and dissemination, technology, and parent-training and information centers.

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] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

2.2.2. 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 name or personal identifier. Communications are sent to all registrants at once, not individuals. All accommodation information is placed in a folder and is retrieved by the folder name, not the registrant's name.

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 118.c.1 National and International Conferences and Conventions
Disposition instructions: TEMPORARY Cut off after end of conference. Destroy/delete 2 years after cutoff or when no longer needed for reference, whichever is sooner.

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

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

For the events website, the system collects the registrant's name, professional affiliation, contact email, and whether they require an accommodation and what type.

For the collaboration and Engage websites, the system collects name and email address. Users may choose to post additional PII however that is not promoted.

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

Yes	IDEA ACDM collects only the minimum information necessary to administer the program. Contact information is needed to register and communicate with individuals for events and meetings, and to register for the collaboration space. Accommodation information is collected so that the accommodations can be provided. Disability information is not collected. No information is collected that is not required to achieve these purposes.

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

Event attendees and those wishing to access the collaboration space register themselves and create an account.

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

Individuals register online on a web page portal.

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?

Users enter their own information. The email field is confirmed so that both the email addresses match and are validated to ensure it is a valid email format.

Use

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

The PII is used to register individuals for events and to allow for access to the collaboration and Engage websites, as well as to make nametags. Accommodation information is also collected so that the Department may ensure access to the events and meetings for those who need it.

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

[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.

No

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

☑ N/A

Click here to enter text.

Social Security Numbers

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

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

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Registrants have access to the website's Privacy Policy when registration is open. This PIA is published on the Department's PIA webpage. There is no additional notice given to the user.

Privacy Policy

The principal activity of the https://collab.osepideasthatwork.org website is to enable OSEP to provide a virtual space for stakeholders to share information and to work together to improve outcomes for children with disabilities.

American Institutes for Research recognizes that users of https://collab.osepideasthatwork.org (the Site) value their privacy. Our goal is to create a safe online environment of trust and community with our users. The following privacy policy discloses our information gathering and dissemination practices for this Site.

1. *What personal information is gathered about you and how do we use it?*

AIR will not disclose any personal information to any third party without your consent, except when necessary in connection with services provided by appropriate intermediaries (e.g., an external vendor assisting with delivery of a product ordered by a customer), who will be required to comply with the confidentiality provisions of this policy.

AIR may gather the following types of information:

- *Information given voluntarily while using a feature of this website, for example, subscribing to a newsletter. We may use your telephone number or email address to contact you if we have trouble processing a registration, etc. However, we will never use your telephone number for sales or marketing purposes.*
- *Information gathered as a result of voluntary participation in a survey or poll, or when communicating with our webmaster or other members of our Web Team.*
- *Information gathered automatically when users visit our website (i.e., IP address, session time [date, time, duration on site], click path analysis, page requests, user's browser and Operating System version).*

Our server will not automatically record your name or email address.

2. *With whom is your information shared?*

AIR may automatically receive and record information on our server logs from your browser, which may include your IP address, session time, click path analysis, and the pages you request.

We will never share, sell, or rent individual personal information with anyone without your advance permission, or unless ordered by a court of law. Information submitted to us is only available to employees managing this information for purposes of contacting you or sending you emails based on your request for information, and to contracted service providers for purposes of providing services relating to our communications with you.

We reserve the right to disclose any content, records, or electronic communication of any kind (including, but not limited to, personal information or private electronic communication transmitted on the Site): (i) to satisfy any law, regulation, or government request; (ii) if such disclosure is necessary to operate our business; or (iii) to protect the rights or property of AIR or its users, sponsors, providers, or licensors. We also reserve the right to reject any order or to request additional information from any user.

3. What about other sites linked from the Site?

Please be aware that when you are on the Site, you can be directed to other sites that we do not control. These other sites may send their own cookies, collect data, or solicit personal information. We are not responsible for the privacy practices of third-party sites.*

** "Cookies" are text files sent from a site's server and stored by your web browser on your computer's hard drive. Cookies allow sites to personalize and save preferences. Cookies can be used to collect anonymous data and serve the user with specifically targeted ads. Most web browsers automatically accept cookies, but you can usually configure your browser to prevent that.*

4.What about information you post on the Site?

If you post information on, or transmit information to other people through, the Site, including without limitation, on message/bulletin boards on the Site, such information will be publicly available and you have no expectation of privacy or confidentiality regarding such information.

5. Confidentiality / Security

We have implemented security policies, rules, and technical measures to protect the personal data that we have under our control from:

- *unauthorized access*
- *improper use or disclosure*

- *unauthorized modification*
- *unlawful destruction or accidental loss*

All our employees and data processors, who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of our visitors' personal data.

6. Access to Personal Data

You can verify the personal data we hold about you by sending an email to osepcollab@air.org(link sends e-mail), although we may require proof of your identity. We will provide the information without charge. We allow you to challenge the data that we hold about you and, where appropriate, you may have the data erased, amended, or completed.

Your Agreement

By using this Site, you acknowledge and agree to this privacy policy. We reserve the right to change, add, or remove all or part of our privacy policy at any time by posting the changes on this page. Your continued use of the Site following the posting of changes to these terms means you accept such changes.

If you have any comments or questions about our privacy policy, please contact us at osepcollab@air.org.(link sends e-mail)

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

Link to the webpage where the notice is posted: https://osepideasthatwork.org/privacy-policy

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?

If an event attendee wishes to opt out, they are able to register in person instead of registering online. Additionally, if a registrant chooses, they could reach out to American Institutes for Research (AIR) and have a member of the meetings team register them without their contact information, circumventing the online registration process.

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.

Yes

What PII will be shared and with whom?
All of the information collected is shared with the contractor (AIR) to provide support to OSERS in its mission.

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

Information is shared to register attendees, make event nametags, communicate with registrants, and ensure appropriate accommodations are in place. Information is also shared so users may access the collaboration space.

External

5.3. 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

5.4. 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

[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.

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

☑ N/A

Click here to enter text.

5.6. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.7. 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.

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

☑ N/A

Click here to enter text.

5.9. 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

Click here to select.

5.10. 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?

The user is entering this information as part of a registration. If they make an error, they can login into their account and make the correction.

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

They can login into their own account and make any needed changes or they could contact AIR (American Institutes for Research) and the changes or corrections can be made.

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

Users are told that once they register that they can return to their account by logging in to access their information for corrections or additions.

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?

AIR's internal network is protected from unauthorized access by firewalls. The network environment—including firewalls, servers, and desktops, are all protected from intrusions and viruses using the latest firewall and advanced malware mitigation solutions.

Access to IDEA ACDM web or database servers are controlled using technical controls that include file system and database permission settings to ensure only authorized individuals. These servers are scanned for vulnerabilities and patched regularly to minimize the chance of a system/data compromise. All servers are configured to forward logs to a centralized log repository that are monitored by security staff to identify misuse or threat actor attempts to compromise systems.

IDEA ACDM servers are located in data centers where physical access is limited to authorized network/system administrators and senior facility staff using electronic card reader systems. The card reader systems are auditable and are provided to IT Operations to inspect access is authorized. All visits to the AIR data are logged and under escort by authorized badged personnel. AIR employs video surveillance to record access inside the data center.

Network and system administrators are required to sign "privileged access agreements" that comprise rules of behavior tailored for staff with elevator privileges. These agreements are signed annually as part of AIR annual auditing requirements.

Multiple levels of authentication are required to access the IDEA ACDM PII. AIR enforces a strong password standard along with a second factor authentication for remote system access. The IDEA ACDM system is not connected to any other data sources and does not share information with any other system.

IDEA ACDM has technical and administrative controls in place that are compliant with the Federal Information Security Management Act (FISMA) and with National Institute of Standards and Technology (NIST) standards. IDEA ACDM also operates under an approved Authorization to Operate.

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.

Security controls are monitored regularly to meet the Department of Education's Cybersecurity requirements. These include access control, system monitoring, weekly system vulnerability scans, monthly database and application scans and annual assessments administered by the Department of Education OCISO.

8. Auditing and Accountability

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

The system owner regularly meets with the contractor to review status reports and attendee reports.

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.

One privacy risk associated with this system is unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud.

The risks are mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.

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