Privacy Impact Assessment

For

Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings (IDEA ACDM)

Date

June 11, 2012

Point of Contact

Melissa Storm

System Owner

Renee Bradley
(202) 245-7277
Renee.Bradley@ed.gov

Author

Sean Hartwell

Office of Special Education and Rehabilitative Services

U.S. Department of Education

1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

   These two websites collectively are used to disseminate information to Office of Special Education Programs (OSEP) grantees and stakeholders at large. http://www.osepideasthatwork.org disseminates materials developed by grantees to a large audience. http://www.osep-meeting.org disseminates conference and meeting logistical information (including materials, information about locations and times of sessions, and names and affiliations of presenters) to attendees of the conference. The **www.osep-meeting.org** website also collects registration information from participants. Names and contact information are collected, but not disseminated. Payment information (for registration fees) is not collected by the website. Participants are sent to PayPal to enter any payment information. The American Institutes for Research never receives or sees this information.

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

   The authority to collect and use this data is derived from the U.S. Department of Education OSEP contract for the Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings (IDEA ACDM). IDEA ACDM is the consolidation of OSEP Communications and OSEP National Meetings. Supports Research to Practice (RTP) in accomplishing tasks related to the implementation of the Part D National programs of the Individuals with Disabilities Education Act (IDEA) meetings and program analysis. Public Law 108-446 IDEA Part D National Activities Section 650-682.

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

   The National Meetings website collects conference attendee information online and retains it within a SQL database. Information collected includes the following fields:

   user_type, grant_number, firstname, lastname, email, degree, title, department, organization, address1, address2, city, state, zipcode, phone, fax, photoRelease, special_needs, dietary_needs, fee, payment_type, card_type, expiration_date, card_name, authorization_code, check_number, check_name, purchase order number, and (check received date)

   The information is not used to link or cross-reference multiple databases.

4. **Why is the information collected?** How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

   The information is collected to support registration and logistics (number of people attending) for the National OSEP Project Directors' Conference held annually. No information is shared, cross-referenced, or made accessible to any other system. The American Institutes for Research does not receive or see any of the financial information entered. That is done through PayPal. Attendees are required to participate in the PD conference as a part of their grant. Therefore, we collect the names of those who have registered.

5. **Social Security Number (SSN).** If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The system does not collect SSNs.

6. **Uses of the Information.** What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

   All information is used by the American Institutes for Research to organize, host, and successfully complete conferences in support of IDEA ACDM National Meetings. Information is gathered to determine whether participants will give a check for registration payment or be directed to PayPal to pay. Information on the numbers of participants is also gathered for logistical purposes, such as determining room size needed. Names and affiliations of participants are used for name badges. The data are not analyzed.

7. **Internal Sharing and Disclosure.** With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

   The information is shared with OSEP. Information shared includes number of people registered and proposals submitted for presentations through osep-meeting.org.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

   No.

9. **Notice.** Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

   The website (https://www.osep-meeting.org) employs a link to the Department of Education's Privacy Policy. No other informational controls mentioned above are implemented at this time.

10. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

    The AIR local area network (LAN), wide area network (WAN), and telecommunications infrastructure, or "general support system," is managed centrally from the company's headquarters in Washington, DC. This includes IT Service desk support of a standard suite of Office applications and e-mail services. The safeguarding and protections of project data are based on a defense-in-depth architecture. Firewalls, VPN's, and secure remote application access platforms and other boundary controls are implemented based on a risk-based approach that adheres to a least privilege access control model. Specific configuration controls are safeguarded on a strict "need-to-know" basis.

    The AIR client-server environment is protected from intrusions, malicious software, denial-of-service attacks, and insider misuse using a combination of administrative, physical, and technical controls. Access to server resources once inside the network is based on a role-based directory service architecture. Host-level security includes antivirus and malware

protection software that is centrally managed to allow for rapid incident response. Access to all project work is based on file/folder level permissions at the project group level.

All AIR enterprise servers are located in separate, secured rooms with access limited to authorized network administration staff. Server rooms at each location are locked at all times with access is restricted to only IT personnel and Facilities Manager utilizing electronic proximity access badges/pass codes to gain entry and video surveillance to monitor access.. Access to the general systems is limited to AIR employees; contract and temporary staff must sign a nondisclosure agreement before being granted a user account. Visitors are accompanied by AIR staff throughout their visit and not allowed access to the internal network.

AIR ensures our office entrances are monitored 24/7 by security personnel in addition to employing extensive video and electronic monitoring systems within our datacenters. Auditing of security logs is conducted periodically to ensure only authorized users continue to access the system in accordance with AIR policy. Multiple levels of authentication are required to access the IDEA ACDM PII. AIR enforces stringent complex password enforcement for network access, combined with a second level of database separate database authentication to provide a defense in depth approach to securing this sensitive data. This system is not tied to any other data sources and does not share information with any other system. Furthermore, AIR disables all unnecessary services on the database server that holds PII, ensuring any attack footprint is reduced accordingly Additionally, utilization of the ASP.NET framework, which includes security controls that validate user input, aids to minimize unauthorized access to the database via the web application logic tier.

A C&A was conducted in January of 2011 with the merging of two websites (National Meeting, Ideas that Work) into a single project (IDEA ACDM). Additional details on data protection are outlined within the IDEA ACDM System Security Plan (SSP) as part of the C & A effort from late 2011. We are submitting the last 10 items in the Plan of Action and Milestones (POA&M) to fully comply with all security controls from the C & A of the IDEA ACDM system. Financial information is not collected directly on the two websites. Users are routed to PayPal for financial information.

11. **Privacy Act System of Records.** Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

    No.

12. **Records Retention and Disposition.** Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

    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.