Privacy Impact Assessment

For

Office of Communications and Outreach On-Line Registration System (cVent Event Solutions)

Date:

January 15, 2012

Point of Contact:

Office of Communication and Outreach (OCO)

Events Services Team

System Owners:

Adrain Walls

Adrian.Walls@ed.gov

Anya Smith

Anya.Smith@ed.gov

Author:

Adrain Walls

Office of Communication and Outreach (0C0)

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.**

   System Name: OCO\cVent Event Solutions

   System Acronym: cVent Event Solutions

   The U.S. Department of Education (ED) conducts several events each year. This system contains records on individuals and contact persons from organizations and individuals that register for participation in selected training workshops, webinars, hearings, meetings and training sessions and events hosted by ED. The Department has obtained an on-line registration system, cVent Event Solutions, that can handle multiple conference and meetings and allow attendees and trainees to register on-line for any of these events. Major functions of this system include RSVP/Decline status for attendees, breakout sessions, adding guest, printing badges and creating custom reports.

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?**

   ED has authority through 20 U.S.C. Section 3412(e) (2) to perform public information functions, including the provision, through the use of the latest technologies, of useful information about education and related opportunities to students, parents, and communities.

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 information being collected is: attendee’s name, organization, business email address, business phone number, business address/zipcode and city.

   The sources of information are: attendee, speaker, exhibitor, president, superintendent, board member and guest.

   The information is collected via website from individuals requesting to register for an event sponsored by or partnership with the Department of Education.

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 so that ED can register attendees/guests for training workshops, webinars, hearings, meetings and training sessions. The registration process is necessary to provide accurate attendance count, allow attendees to sign up for breakout sessions/tours/receptions and to provide our Department of Education clients with realtime reports. The reports include the contact name, work email address, state, registration count, breakout sessions and any attendee who may need special accommodations.

   The type of data collected includes contact information such as business email, business address/phone and attendees name in order to register them for an event. The software allows for us to create and run several events at the same time. Typically the information disseminated to the attendees is the invitation, confirmation and agenda emails and ED outreach events in a community and other information (agenda, briefing, hearings documents) deemed pertinent by senior leadership. We also collect addresses in order to understand the demographics of those interested in ED's program, conferences and events. Although there is a small risk in collecting this data, it has been properly mitigated with security and data handling measures as discussed below.

The Office of Communications and Outreach is responsible for overall leadership for the Department in its communications and outreach activities, designed to engage the general public as well as a wide variety of education, community, business, parent, academic, student, and other groups, including the media, intergovernmental and interagency organizations, and public advocacy groups in the President's and Secretary's education agenda.

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.**

   No Social Security Numbers are collected.

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.**

   As stated above, the information is collected so that ED can register attendees/guest for training workshops, webinars, hearings, meetings and training sessions. The registration process is necessary to provide accurate attendance count, allow attendees to sign up for breakout sessions/tours/receptions and to provide our clients with real time reports.

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?**

   This information would be shared with ED Point Of Contact (POC) who requested the on-line registration system and event logistic assistance. The contact list is exported to an MS Excel report as requested. Also, the software allows for badges/certificates to be created for the attendees. We do not plan to release the information externally.

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?**

   This information is not shared externally with individuals or organizations.

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?**

Attendees will only be added to the on-line registration system database if they come to the website to register for an event. At the home screen, attendees providing information are notified that they are being added to the contact list and have the option to opt-out receiving additional information.

10. **Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.**

    The privacy note will reside at https://app.cvent.com/Subscribers/Login.aspx

11. **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?**

    This service is currently under the C&A process with OCIO\IA office.

    Some of the security features for cVent include:

    Data hosted in **top-tier, world-class data center**

    Biometric access screening to gain access to cVent servers

    Fire detection and suppression systems

    Fault tolerant, redundant servers

    Data encrypted and transmitted via Secure Socket Layers (SSL) technology

    Hourly backups of customer data stored in different geographic locations

    Full-time staff of physical and network security personnel

    Unique account/username/password access control

    One-way encryption for all passwords

    Account lockout and password expiration

    Proprietary security model

12. **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?

    A system of record notice is not needed because the information collected is not retrieved by any personal identifiers. Therefore, a system of record as defined by the Privacy Act is not being created and the reporting requirements of OMB Circular A-130 do not apply. This information is not retrieved by a personal identifier. The data is dumped for each event and is associated with the event they registered for.

13. **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:**

    Records are covered under ED 144.a. These records are destroyed when no longer needed for reference purposes, or according to a predetermined time period.