



Privacy Impact Assessment
For the Investing in Innovation (i3) Fund

Date: January 26, 2010

Point of Contact: Alula Asfaw

System Owner: James H. Shelton

Author: Alula Asfaw

Office of Innovation and Improvement
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.

The U.S. Department of Education's (ED) Office of Innovation and Improvement (OII) has developed a web-based platform, the Open Innovation Web Portal (Portal), to support communication and collaboration among a wide range of key education stakeholders, including practitioners, funders, and the general public. This platform will allow geographically dispersed but like-minded individuals to discover each other and work together to address some of the most intractable challenges in education. OII plans to promote this platform as a tool for use with the Investing in Innovation grant program (i3), which was established as the "Innovation Fund" in the "American Recovery and Reinvestment Act of 2009" (ARRA), signed into law by the President on February 17, 2009.

The Open Innovation Web Portal will create an ecosystem for educational innovation by:

- *Convening* stakeholders across current network, financial, geographic, or other barriers
- *Encouraging* stakeholders to coordinate efforts, share knowledge, and invest strategically.
- *Facilitating* idea generation and refinement, access to funders, and partnerships between individuals/organizations.
- *Highlighting* consumer needs and innovations in the community.

This platform will consist of two parts: (1) Using web-based community brainstorming and collaboration to generate and improve innovative ideas; and (2) Facilitating communication among innovators, funders, and education practitioners (teachers, schools, and districts) from across the country. This platform will be an important mechanism for identifying and scaling promising and proven ideas.

Although the web portal will not have a formal connection to the i3 Fund, it will be an important signal of the Department of Education's commitment to innovation and is expected to serve as an important *informal* tool for potential applicants to refine their ideas, coordinate partnerships and funding opportunities. Thus the portal will support our i3 efforts by improving the quality, quantity, and support for i3 proposals.

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 Department of Education has entered into a Memorandum of Understanding with VenCorps authorized under 20 U.S.C. § 3475. The web portal initiative is granted legal authority under section 14007 of the Investing in Innovation Fund as a part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). This initiative also has legal authority under section 20 U.S.C. § 3412 (e) (2) which gives the Department general authority to perform "public information functions, including the provision through the latest technologies, of useful information about education and related opportunities to students, parents, and communities."

3. **Characterization of the Information.** What elements of 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 the

information is collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

Data Collected:

The website application neither requires nor collects any personal information other than first name, last initial, city, state, zip code, and email address [private] -- we do not collect street addresses, telephone numbers, social security numbers, or any financial information. Users are identified to each other via first name as well as a user selected unique username -- not via any externally meaningful identifier.

The system will collect and maintain the user's first name and last initial and e-mail address [private]. However, the e-mail address will not be made publically available. When an individual voluntarily posts information about his or her idea in the portal and a foundation reviewing the posted information wants to correspond with that individual, the foundation will click the "send comment" button. The person sending the information and the person receiving the information will not have access to personally identifiable information of the other user. It is important to note the information that is collected and maintained on the portal system is not verifiable, linkable to a specific user/participant on the portal and is not cross referenced to any other database.

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 type of data collected, discuss the privacy risks identified and how they were mitigated.

The web portal initiative is central to the i3 fund specifically and to the innovation strategy of the Department of Education generally. The web portal will allow us to involve many more teachers, parents, and many others who care about educational issues to find important solutions to the most persistent challenges in education. The Department is also dedicated to using technology to help spur innovation in the sector.

Aggregate information is collected for 2 reasons: (1) Facilitate collaboration and networking between individuals and organizations in the field (e.g., helping them to find potential partners to improve ideas); and (2) Improve the functionality of the web portal.

There is no evidence of privacy risks to the user because the information that will be collected by ED and VenCorps will be aggregate data that is not linked to any individual user of the web portal.

The controls identified under Question 10 (Security) address the administrative, physical, and technical controls required to secure, protect, and preserve the confidentiality of any information in identifiable form from privacy risks.

5. Social Security Numbers - 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.

SSNs are not 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? If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

The Department of Education and VenCorps will not collect or otherwise use any personally identifiable information posted by participants of the web portal. The Department will only use aggregate, data that is not linked to any individual to help improve the system and measure success of the portal. The information will only be analyzed for these two purposes by OII and VenCorps.org. The system will also not use any commercial information. The aggregate data collected will not be shared.

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? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

The aggregate data will not be shared with any other parties outside of ED and VenCorps.org. The aggregate data shared will help improve the system and measure the success of the portal to involve many more teachers, parents, and many others who care about educational issues to find important solutions to the most persistent challenges in education.

There is no evidence of privacy risk to the user because the information that will be shared by ED and VenCorps will be aggregate data that is not linked to any individual user of the web portal.

OII is taking further steps to protect the users' information by limiting access to the data to senior members of both OII and VenCorps.org.

The controls identified under Question 10 (Security) address the administrative, physical, and technical controls required to secure, protect, and preserve the confidentiality of any information in identifiable form from privacy risks.

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? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Pursuant to the Memorandum of Understanding between ED and the web-based platform host VenCorps, no information is shared with an external entity.

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?

A privacy policy to be developed by ED will appear with a link on the webpage to give to get explicit agreement from participants. The policy will provide notice to individuals about how the data is used, and highlights the voluntary nature of information collected.

If a user voluntarily provides sensitive personally identifiable information (i.e., SSN), not requested, then, this information is flagged and removed from the portal. The flagging process allows the Department of

Education team that manages the site know that there has been sensitive information posted and allows us to contact the user.

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 innovation.ed.gov portal and its hosting arrangements have been designed and implemented to protect the privacy of participants in this educational innovation community.

The Department has determined that the risk of breach is minimal because of specific administrative, physical and technical safeguards.

Technical Security:

The application and database servers are hosted on the IBM Cloud Service, behind firewalls configured to meet the needs of the financial services industry. The network and servers have 24x7 security and operational monitoring by IBM Global Services personnel. The Portal servers run on dedicated server instances on virtual hosts, using storage dedicated to those hosts. All access to the servers, once in production will be encrypted; web access will be via port 443 SSL only; administrative access is limited to SSH access requiring an IBM issued digital certificate. Database backup files will be encrypted prior to being transferred to offsite facilities for disaster recovery.

Physical Security:

All production application data is stored on database servers hosted by IBM in its Poughkeepsie, NY data center, being replaced around 25-Jan-2010 by the facility in Southbury, CT. Access to the 230-acre site is restricted to authorized personnel only. It has 250,000 square feet (23,000 m²) of "raised floor" data center space. It is an "off the grid" facility, with its power plant taking advantage of jet turbine technology to generate power for the entire site.

Administrative Processes:

Administrative access to the production servers is limited to senior members of the Portal development and support team. Application administration will be limited to those individuals designated by Department of Education and VenCorps senior management for that purpose. All access logs are retained, providing an audit trail of all administrative activities on the system.

Access to computerized records is limited, through use of access codes and entry logs, to those whose official duties require access. All physical access to the Department site, and the sites of Department contractors where this system of records are maintained, is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge. Is the system compliant with any federal security requirements?

The "Open Innovation Web Portal" has been categorized as a Low-risk impact system in accordance with NIST FIPS 199. The certification and accreditation (C&A) of the system is underway and will be completed before the system goes operational.

The 'Open Innovation Web Portal' complies with all federal and departmental information and technology security requirements.

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?

A Privacy Act System of Records is not being created. The posts by participants to the web portal are anonymous and are tracked in aggregate form and will never be identified with or lead back to any individuals.

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:

There is no NARA-approved records retention schedule for the Open Innovation Web Portal. These records will be treated as permanent records until a schedule is approved.