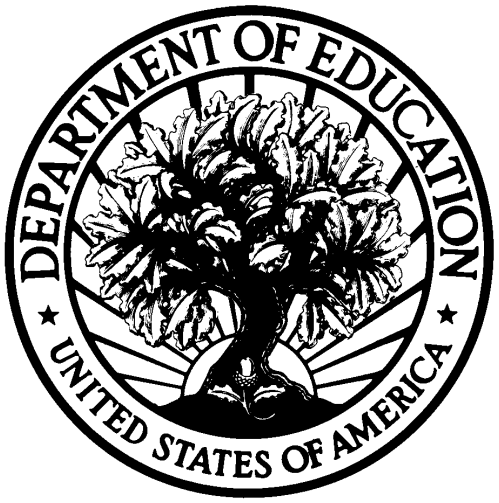

Privacy Impact Assessment

For

Impact Evaluation of Upward Bound's Increased Focus on Higher-Risk Students

Date

June 15, 2007

System Owner:

Dr. Ricky Takai

Office of Institute of Education Sciences
U.S. Department of Education

1. What information will be collected for the system?

The system of records will include information about sampled students, including their names, addresses, demographic information such as race/ethnicity, gender, age, and educational background, attitudes toward school, and educational aspirations.

2. Why is this information being collected?

The information in this system is used for the following purpose: To study, as authorized by section 402H of the Higher Education Act of 1965, as amended (HEA), 20 U.S.C. 1070a-18, the impacts of Upward Bound on eligible students' preparation for, and success in, postsecondary education. In particular, this system is necessary to provide information for analyses of the impacts of the Upward Bound programs on higher-risk students as well as on other eligible students. The system is also needed for analyses of variations in impacts on students according to the characteristics of Upward Bound projects and control group students' access to, and receipt of, services similar to those offered through Upward Bound.

3. How will the information be used?

The system will contain information about approximately 3,600 students applying for admission at approximately 90 Upward Bound grantees for the 2007-2008 academic year, of which approximately 1,800 will have been offered admission to Upward Bound and 1,800 will serve as a control group for the purposes of this evaluation. These students will be in either 9th or 10th grade during the 2007-2008 academic year. The Upward Bound grantees included in the evaluation will be a sample of all Upward Bound grantees.

4.Will this information be shared with any other agency or entity? If so, with which agency or agencies/entities?

Information is disclosed internally to administer the program. However, it is not shared externally, except as required by law, or under the routine uses listed in the Privacy Act System of Records notice. These disclosures may be made on a case-by-case basis, or if the Department has complied with the computer matching requirements of the Act, under a computer matching agreement. Such disclosures may include: for litigation purposes, to the Department of Justice for FOIA advice, to contractors conducting Department business, for law enforcement, to a member of Congress at the request of the data subject, or to a consumer reporting agency regarding a valid and overdue claim.

5. Describe the notice or opportunities for consent that would be or are provided to individuals about what information is collected and how that information is shared with other organizations.

There is not notice or opportunities for consent since information is provided voluntarily.

6. How will the information be secured?

All physical access to the Department's site, to the sites of the Department's contractor, and to the sites of the subcontractors where this system of records is maintained, will be controlled and monitored by security personnel. The computer system employed by the Department

offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a ``need to know'' basis, and controls individual users' ability to access and alter records within the system.

The contractor selected for this evaluation has been required to establish similar sets of procedures at its sites and at subcontractor sites to ensure confidentiality of data. Their systems will be required to provide reasonable assurance that information identifying individuals is in files physically separated from other research data. The contractor and subcontractors are required to maintain security of the complete set of all master data files and documentation. Access to individually identifiable data will be strictly controlled. At each site all data will be kept in locked file cabinets during nonworking hours, and work on hardcopy data will take place in a single room, except for data entry. Physical security of electronic data will also be maintained. Security features that protect project data include password-protected accounts that authorize users to use the contractor's and subcontractors' information systems but only to access specific network directories and network software; user rights and directory and file attributes that limit those who can use particular directories and files and determine how they can use them; and, additional security features that the network administrators establish for projects as needed. The contractor and subcontractor employees who ``maintain'' (collect, maintain, use, or disseminate) data in this system shall comply with the requirements of the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573).

In safeguarding personally identifiable information (PII), the contractor and its subcontractors also are subject to the Department's requirements contained in the Department of Education's Handbook for the Protection of Sensitive But Unclassified Information, OCIO-15, and the Department's policy that the transmission of sensitive but unclassified information, including PII, through an e-mail requires that the contents be password protected in a ZIP file.

7. Is a system of records being created or updated with the collection of this information?

The system is covered under the system of records notice Impact Evaluation of Upward Bound's Increased Focus on Higher-Risk, dated June 15, 2007, (72 FR 33213-33215)