Privacy Impact Assessment
for the
TRIO Programs Annual Performance Report (APR) System

Date
May 20, 2008

Contact Point
System Owner and Author: Frances Bergeron, Team Leader, Program Management and Development, Federal TRIO Programs

Office of Postsecondary Education

U.S. Department of Education

1. What information will be collected for the system?

The TRIO Programs Annual Performance Report (APR) System collects individual student records on individuals served by the following Federal TRIO Programs: Upward Bound (which includes regular Upward Bound (UB), Upward Bound Math-Science (UBMS), and Veterans Upward Bound (VUB)); Student Support Services (SSS); and the Ronald E. McNair Post baccalaureate Achievement (McNair) programs.

The individual student records include personally identifiable information such as social security number (SSN), name, date of birth, as well as information on each individual's eligibility for services and the student's academic progress.

2. Why is this information being collected?

The information contained in this system is being collected to assist in monitoring grantee performance and to determine program outcomes in response to the requirements of the Government Performance and Results Act (GPRA) and the OMB Program Assessment Rating Tool (PART) process. GPRA does not specifically require the collection of individual participant records with personal information. However, to determine if the goals of the programs are being met, the academic progress of program participants must be tracked over multiple years. Collecting individual participant data, including the SSN, is the most reliable method for matching records across years needed to determine program effectiveness. Although the collection of the SSN is not required by statute, it serves a distinct business need of the Department. The SSN serves as the unique identifier for matching participant records across years. Although another unique identifier might be used for the APRs, the SSN is needed to match the APR data with other databases, such as the Federal Title IV (financial aid) Applicant and Recipient File and the National Student Clearinghouse. Matching with these other databases can supplement APR information on postsecondary enrollment, persistence, and completion. Further, there would be substantial administrative costs to project grantees to implement another unique identifier for program participants. Most project grantees are institutions of higher education that already collect SSNs for all students applying for Federal financial aid.

3. How will the Department of Education use this information?

The Department uses the data collected to (a) evaluate projects' accomplishments, (b) determine the number of prior experience points to be awarded to current grantees, (c) aid in compliance monitoring, and (d) demonstrate program effectiveness.

The information that grantees submit in the performance report allows the Department to assess annually each grantee's progress in meeting the project's approved goals and objectives. The performance report data are compared with the project's approved objectives to determine the project's accomplishments, to make decisions regarding whether funding should be continued, and to award "prior experience" points for meeting approved objectives. For some of the program objectives (e.g., percentage of participants enrolling in postsecondary education), a grantee must track the academic progress of participants for several years (e.g., for a student first served as a high school freshman, it will be four or more years before it is known if the student enrolls in postsecondary education).

In addition, the Department uses the annual performance reports (APRs) to produce program-level data for annual reporting and program profile reports, budget submissions to OMB, Congressional hearings and inquiries, and responding to inquiries from higher education interest groups and the general public. By collecting individual participant records, the data is submitted in a consistent format and can be easily aggregated to demonstrate program outcomes needed for the Department's response to the requirements of the Government Performance and Results Act (GPRA).

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

Two separate Department contractors have access to the data: (1) the contractor responsible for the data collections, and (2) the contractor(s) responsible for the data analysis. Except as noted below, only select Department staff and the contractors have access to the data that is used primarily to administer the programs and report program outcomes as noted above. Occasionally the data is shared with the Office of the Inspector General (OIG) in the conduct of official investigations.

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.

Institutions of higher education and agencies that receive grants under the UB, SSS, and McNair programs are required to submit an annual performance report (APR). The OMB approved APRs for these three programs require grantees to submit participant-level data on each individual served. In collecting the data required by the APRs, the grantee institution/agency follows the Privacy Act regarding consent.

These programs compliment the Federal financial aid programs that also require the collection of personal identifying information such as SSN, name and birth date.

In addition, the following statement is provided on the OMB approved APRs for each of these three programs:

> In accordance with the Privacy Act of 1974 (Public Law No. 93-579, 5 U.S.C. 552a), you are hereby notified that the Department of Education is authorized to collect information to implement the Upward Bound [Student Support Services; Ronald E. McNair Post baccalaureate Achievement] program under Title IV of the Higher Education Act of 1965, as amended (Pub. Law 102-325, Sec. 402D). In accordance with this authority, the Department receives and maintains personal information on participants in the Upward Bound [Student Support Services; McNair] program. The principal purpose for collecting this information is to administer the program, including tracking and evaluating participant progress. Providing the information on this form, including a social security number (SSN) is voluntary; failure to disclose a SSN will not result in the denial of any right, benefit or privilege to which the participant is entitled. The information that is collected on this form will be retained in the program files and may be released to other Department officials in the performance of their official duties.

6. How will the information be secured?

Since the data a grantee submits contains confidential information on participants, a grantee must submit the participant data via a secured Website that meets the Department of Education's (Department) rules and standards for security of sensitive data. The data reside in a secured facility on a secured server behind a Department approved firewall system that continuously monitors for intrusion and unauthorized access. The IT contractor security staff is notified of Windows security updates and views server security status reports and applies updates as needed and uses anti-virus software on all servers and workstations.

The data collection site requires grantees to log in with a Department issued login ID and password. All screens and data transfers are encrypted and transmitted using HTTPS protocols. The IT contractor transfers the data to the analysis contractor via a secured FTP site. As with the IT contractor, the data analysis contractor’s security program is compliant with federal government regulations and NIST standards.

Only contractor staff that supports the data collection or data analysis and a small number of Department staff are allowed access to the data. Contractor staff has

appropriate security clearances and also signs confidentiality and non-disclosure agreements to protect against unauthorized disclosure of confidential information.

Certification and Accreditation (C&A) is used to ensure that information systems have adequate security commensurate with the level of risk. The certification is a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards (e.g., physical, personnel, procedural, and environmental) to establish the extent to which a particular design and implementation meet a set of specified security requirements. The accreditation is a formal declaration by a Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. The TRIO Programs APR System complies with the Department's C&A policy.

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

Yes, a system of records is being created with the collection of this information.