Privacy Impact Assessment (PIA)
for the

TRIO Programs Annual Performance Report (APR) System

Jan 23, 2018

This PIA was approved on May 20, 2008 and reviewed on Nov 21, 2017 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Kathy Morgan

Contact Email: kathy.morgan@ed.gov

System Owner

Name/Title: Joyce Fitzgerald

Program Office: Office of Postsecondary Education (OPE)

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. **If a question does not apply to your system, please answer with N/A.***

All text responses are limited to 2,000 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 ☐ N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

The TRIO Programs Annual Performance Report (APR) System, an existing 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 [UMBS], and Veterans Upward Bound [VUB]), Student Support Services (SSS), and the Ronald E. McNair Postbaccalaureate Achievement Program (McNair).

1.2 ☐ N/A Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

The PII in the system is being collected to assist in monitoring grantees' performance and to determine program outcomes in response to the requirements of the Government Performance and Results Act (GPRA).

1.3 ☐ N/A Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 ☐ N/A Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

Updated PIA Original Publication Date: 05/20/2008

1.5 ☐ N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1 ☐ N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

The legal authority to collect and use this data is derived from Title IV of the Higher Education Act of 1965, as amended (Pub. Law 102-325, Section 402D). In accordance with this authority, the Department receives and maintains personal information in the TRIO programs cited in 1.1.

[1] The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

SORN

2.2 ☐ N/A Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer **YES** or **NO**.

Yes

2.2.1 ☐ N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name and number, or indicate that a SORN is in progress.

The TRIO SORN (18-12-07) is currently being updated. The last fully published version was posted in the Federal Register on January 23, 2009 at 74 FR 4165.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov.

2.3 ☐ N/A Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

The records disposition schedule is ED 254: Grant Administration and Management Files. Disposition: Temporary, Destroy/Delete 10 years after final action is taken on file, but longer retention is authorized if required for business use. The records schedule number is N 1-441-11-00 1.

2.4 ☐ N/A Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

3.1 ☐ N/A List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

The individual student records include personally identifiable information such as social security numbers, names, and dates of birth, as well as information on each individual's eligibility for services and the student's academic progress. The information is collected online; the data is used both for a specific year and as part of the specific program's longitudinal file.

3.2 ☐ N/A Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

3.3 ☐ N/A What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

The TRIO programs' grantees collect the PII directly from participants in the program, or from a participant's parent(s). Grantees are most typically institutions of higher education or public or private agencies or organizations.

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

3.4 ☐ N/A How is the information collected from stated sources (paper form, web page, database, etc.)?

The information is collected online, via a Web site, and moved to a database.

3.5 ☐ N/A How is this information validated or confirmed?[3]

The project director and certifying official of each institution submitting an APR must certify the accuracy and completeness of all information in the report. Grants are awarded for five-year periods. Every year, TRIO's data analysis contractor merges the APR data with previous years' data; the program achieves a match to older records in a very high percentage of cases (excluding cases first reported in the APR that would not have a prior record).

Use

3.6 ☐ N/A Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

GPRA does not specifically require the collection of individual participant records with personal information. However, to determine whether the goals of the programs are being met, the academic progress of program participants must be tracked over multiple years. The SSN serves as the unique identifier for matching participants' 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 National Student Loan Data System (NSLDS). Matching with these other databases can supplement APR information on postsecondary enrollment, persistence, and completion.

3.7 ☐ N/A Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1 ☒ N/A If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

Enter text here.

3.8 ☐ N/A Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 ☒ N/A If the above answer is **YES,** please explain.

Enter text here.

[3] Examples include form filling, account verification, etc.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.9 ☐ N/A Does the system collect Social Security Numbers? Please answer **YES** or **NO**.

Yes

[3] Examples include form filling, account verification, etc.

3.9.1 ☐ N/A If the above answer is **YES,** explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

Collecting individual participant data, including the SSN, is the most reliable method for matching records across years needed to determine the TRIO programs' effectiveness. Although collecting SSNs is not required by statute, it serves a distinct business need of the Department--to match participants' data across years, and to match that data with other highly relevant databases.

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 the programs' effectiveness. The information that grantees submit in the APR 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 APRs to produce program-level data for annual reporting and program profile reports, budget submissions to OMB and Congressional hearings, and responses 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 GPRA.

3.10 ☐ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

TRIO staff members have noticed over the past several years that some current grantees (largely institutions of higher education) have decided not to provide SSNs in their annual performance reports. Moreover, TRIO has investigated the possibility of successfully tracking participants over time through methods not involving SSNs. During the next few years, TRIO staff members and contractors will implement a phase-out plan using unique, randomly generated case numbers in place of SSNs.

4. Notice

4.1 ☐ N/A How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

Institutions of higher education and agencies that receive grants under the UB, SSS, and McNair programs are required to submit APRs. The OMB-approved APRs for these three programs require grantees to submit participant-level data on each individual served. In collecting the data thus required, the grantee institution/agency follows the Privacy Act regarding consent, as noted in the question 4.2, directly below.

4.2 ☐ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

The following statement is provided in the OMB-approved APR data collection instruments to which grantees respond:

Note to the Data Collector: When you collect this information from participants, please make sure that you inform them why they are being asked to provide Social Security numbers. Please see Privacy Act Statement below and convey its content to students and parents as you collect the information.

Privacy Act Statement - 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, including Social Security numbers (SSNs), to implement the Upward Bound program under Title IV of the Higher Education Act of 1965, as amended (Pub. Law 102-325, sec. 402A and 402C). In accordance with this authority, the Department receives and maintains personal information on participants in the Upward Bound program. The principal purpose for collecting this information is to administer the program, including tracking and evaluating participants' academic progress. Your SSN is collected only to serve as the unique identifier for matching participant records across years. Providing the information on this form, including a SSN, is voluntary; failure to disclose a SSN will not result in 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 official duties. The information will not be disclosed outside of the Department, except as allowed by the Privacy Act of 1974, pursuant to the routine uses identified in the System of Records Notice titled "TRIO Programs Annual Performance Report (APR) System (TRIO APR)."

4.3 ☐ N/A What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

While each grantee institution that receives a grant under the UB, SSS, or McNair programs is required, without exception, to submit an APR with data on each individual served, a specific participant in a grant projects, or the participant's parents, may decline to provide information for the data fields in the APR, as indicated in the Privacy Act statement in question 4.2 above. Any participant may opt out of the project at any time.

5. Information Sharing

Internal

5.1 ☐ N/A Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2 ☐ N/A What information will be shared and with whom?

Two separate Department contractors have access to the data: (1) the contractor responsible for the data collections, and (2) the contractor responsible for the data analysis. Select Department staff (for example, the Office of the Inspector General in the conduct of official investigations) and the contractors have access to the data that is used primarily to administer the programs and report program outcomes, as noted below.

For Upward Bound (UB) and Upward Bound Math-Science (UBMS), TRIO has submitted APR data, including SSNs, to the office of Federal Student Aid, using secure transmission, so that the data can be matched to the National Student Loan Database System, thus providing TRIO with additional information on the extent to which UB and UBMS participants have enrolled in postsecondary education.

5.3 ☐ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Please see question 5.2. The purpose does align with the stated purpose in Question 1.2.

External

5.4 ☐ N/A Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

No

5.5 ☐ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

5.6 ☐ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

5.7 ☐ N/A How is the information shared and used by the external entity?

5.8 ☐ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

No

5.9 ☒ N/A Does the project place limitation on re-disclousre? Please answer **YES** or **NO**.

6. Redress[4]

6.1 ☐ N/A What are the procedures that allow individuals to access their own information?

Please refer to the SORN for information on record access procedures. https://www2.ed.gov/notices/sorn/18-12-07_012309.pdf

6.2 ☐ N/A What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Please refer to the SORN for information on contesting record procedures. https://www2.ed.gov/notices/sorn/18-12-07_012309.pdf

6.3 ☐ N/A How does the project notify individuals about the procedures for correcting their information?

Please refer to the SORN for information on notification procedures. https://www2.ed.gov/notices/sorn/18-12-07_012309.pdf

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1 ☐ N/A Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer **YES** or **NO**.

Yes

7.2 ☐ N/A What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

Since the data a grantee submits contains confidential information, a grantee must submit the participant data via a secured Web site that meets the Department's rules and standards for security of sensitive data. Up until fall 2017, the data resided in a secured facility on a secured server behind a Department-approved firewall system that continuously monitored for intrusion and unauthorized access. In the fall of 2017, the data hosting contractor migrated the data to the Amazon Web Service (AWS) Federal Risk and Authorization Management Program (FedRamp) certified cloud. All screens and data transfers are encrypted and transmitted using HTTPS protocols. The data hosting contractor transfers the data to the analysis contractor via a secured FTP site.

7.3 ☐ N/A What administrative, technical, and physical safeguards are in place to protect the information?

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

Up until fall 2017, the data resided in a secured facility on a secured server behind a Department-approved firewall system that continuously monitored for intrusion and unauthorized access. In the fall of 2017, the data hosting contractor migrated the data to the Amazon Web Service (AWS) Federal Risk and Authorization Management Program (FedRamp) certified cloud. All screens and data transfers are encrypted and transmitted using HTTPS protocols. The data hosting contractor transfers the data to the analysis contractor via a secured FTP site. As with the data hosting contractor, the data analysis contractor's security program is compliant with Federal government regulations and NIST standards.

7.4 ☐ N/A Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 ☐ N/A Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

Yes

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

7.6 ☐ N/A Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 ☐ N/A Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 ☐ N/A Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

Up until fall 2017, the data resided in a secured facility on a secured server behind a Department-approved firewall system that continuously monitored for intrusion and unauthorized access. In the fall of 2017, the data hosting contractor migrated the data to the Amazon Web Service (AWS) Federal Risk and Authorization Management Program (FedRamp) certified cloud. All screens and data transfers are encrypted and transmitted using HTTPS protocols. The data hosting contractor transfers the data to the analysis contractor via a secured FTP site.

8. Auditing and Accountability

8.1 ☐ N/A How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

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. OPE employees who access the data have appropriate security clearances. Contractors and Departmental employees are required to complete annual mandatory security awareness and privacy act training.

8.2 ☐ N/A What are the privacy risks associated with this system and how are those risks mitigated?

Security Assessments and Authorizations are used to ensure that information systems have adequate security commensurate with the level of risk. The assessment and authorization are 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 authorization is a formal declaration by an Authorizing Official 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 APR complies with the Department's Security Assessment and Authorization policy.

Up until fall 2017, the data resided in a secured facility on a secured server behind a Department-approved firewall system that continuously monitored for intrusion and unauthorized access. In the fall of 2017, the data hosting contractor migrated the data to the Amazon Web Service (AWS) Federal Risk and Authorization Management Program (FedRamp) certified cloud.