# Privacy Impact Assessment (PIA)

for the

# TRIO Programs Annual Performance Report (TRIO APR) System

# September 2, 2022

**For PIA Certification Updates Only:** This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

## Contact Point

**Contact Person/Title:** Emory Morrison/Director, Student Program Development Division
**Contact Email:** Emory.Morrison@ed.gov

## System Owner

**Name/Title:** Joyce Fitzgerald/Management and Program Analyst
**Principal Office:** Office of Postsecondary Education

**Please submit completed Privacy Impact Assessments to the Privacy Office 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.***

## 1. Introduction

**1.1.** Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Federal TRIO[1] programs fund projects that provide services to individuals who meet both first-generation (FG) college student and low-income (LI) standards and are pursuing a college degree. Different TRIO programs fund projects that serve individuals who are at different points along their pathway towards a college degree. While FG/LI status is a common criterion to be eligible for service by a TRIO project, some TRIO programs include additional criteria.

The Federal TRIO programs require funded projects to submit annual performance reports (APRs) to the U.S. Department of Education (Department) that include information sufficient to calculate metrics related to performance targets. The Department maintains a TRIO APR data collection system (TRIO APR) that hosts six APR data collections, four of which are for projects within programs that submit individual level records (on students or veterans) as part of their APR data collection. The four TRIO APR data collections that include individual level data are for (1) Student Support Services (SSS) projects, (2) Ronald E. McNair (McNair) Postbaccalaureate Achievement projects, (3) Upward Bound/Upward Bound Math-Science (UB/UBMS) projects, and (4) Veterans Upwards Bound (VUB) projects. The two remaining TRIO APR data collections only require submission of aggregated data.

Projects[2] funded within those four programs use a secure data collection system (a web-based application hosted on a FedRAMP-certified cloud server (AWS)) to submit records on students or veterans, depending on the collection, that were served in a project year, and on individuals that had been served in prior project years who are having their academic progress tracked across multiple years so that academic

[1] "TRIO" is a term that was established in 1965 by the Higher Education Act of 1965 to refer to the first three programs that were established in that year. In subsequent years, the number of TRIO programs has increased, but the established term TRIO continues to be used to refer to the set of programs with the common mission and administration. The term is not an acronym.

[2] SSS grant projects are institutions of higher education (IHE) that offer either a two-year degree, a four-year degree or both; McNair grant projects are institutions of higher education that offer four year degrees; Upward Bound grant projects (including UB, UBMS, and VUB projects) may be an IHE or a non-profit organization that offers community services.

persistence and degree attainment goals can be evaluated. The TRIO APR system also includes a Microsoft Structured Query Language (SQL) Server for database support and a Microsoft web server.

The system collects APR information from TRIO grant projects as submitted by the project. The system packages together information into two primary data products: (1) APR collection databases (in MS Access format), and (2) Project APR summary data files (in PDF format).

The system generates the summary data files in real time as projects submit their data. Grant projects are required to download the PDF file that the system generates, securely store the document as part of their required grant project record keeping, and formally certify that they have reviewed the document and that the information is accurate.

The contractor that operates the system packages the summary data files, downloads the files into a secure Department internal directory, and shares this directory with the program office. The PDF files are then uploaded into appropriate locations within the G5 grants management system, where a specialist from the program office can access the files.

The summary data files are password-protected and stored in a directory location (outside the system boundary) with limited and privileged user access. Access privileges to this directory location are restricted to staff in the program office and select staff from the contract team. Collectively, the number of individuals with access privileges to this location number fewer than ten. All files within this directory with PII are password protected.

**TRIO APR Collections that maintain Individual-Level Data**

The SSS program funds projects, typically institutions of higher education (IHEs), that provide programming and services (e.g., mentoring, tutoring, financial literacy training) to serve individuals who are enrolled within the IHE. SSS programming is designed to promote postsecondary persistence and degree attainment. The SSS APR data collection includes individual identifiers (name and date of birth), basic demographic information[3] and information regarding academic standing while the students are being served, enrollment, persistence, college transfer, and degree attainment. Grant projects track and report on individuals for four to six years after they had been first served by a grant project in order to assess degree attainment.

[3] Demographic information includes race, sex, and information related to meeting service eligibility requirements (such as status relative to family low-income thresholds, and status relative to parental educational attainment).

The McNair program serves individuals who are enrolled in postsecondary education and have expressed an interest in pursuing a research doctoral degree. The McNair APR data collection includes basic demographic information and information regarding academic standing while the students are being served, research experiences supported as part of participation in the project, enrollment, persistence, and degree attainment. Grant projects track and report on individuals for ten years after the student receives their bachelor's degree by a grant project to assess progress toward doctoral degree attainment.

The UB and UBMS programs serve students while they are enrolled in secondary school. The UB and UBMS APR data collection includes basic demographic information and information regarding academic standing while the students are being served, enrollment, persistence, and degree attainment. Grant projects track and report on individuals for six years after enrollment in postsecondary education to assess postsecondary degree attainment. For UB and UBMS, TRIO submits APR data to the office of Federal Student Aid (FSA), using secure transmission, so that the data can be matched to the National Student Loan Database System (NSLDS), providing TRIO with additional information on the extent to which UB and UBMS participants have enrolled in postsecondary education.

The VUB program serves veterans who are interested in enrollment in postsecondary education. The APR data collection includes basic demographic information and information about academic history prior to entry into the program, postsecondary enrollment, persistence, and degree attainment for veterans who complete their VUB program. Grant projects track and report on individuals for six years after they complete the program to assess postsecondary degree attainment. The website is hosted in a FedRAMP-certified Amazon Web Services GovCloud environment.

There are no direct connections into or out of the system, although there are regular exports and imports to/from the G5 system performed via a combination of manual steps on a regular basis (e.g., once per year someone accesses G5, searches for a list of new grants in this system's programs, exports it to an Excel spreadsheet, and then manually imports that spreadsheet into the TRIO APR system).

**1.2.** Describe the purpose for which the personally identifiable information (PII)[4] is collected, used, maintained or shared.

[4] 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. OMB Circular A-130, page 33

PII is collected, maintained, and used so that the Department can fulfill its administrative and research requirements associated with the oversight and management of the Federal TRIO programs. The purpose of the Federal TRIO programs is to promote academic persistence and degree attainment for participants served by TRIO grant projects. While data collections occur within annual cycles, many academic persistence and degree attainment goals have considerably longer time horizons than just one year. In order to evaluate and assess performance against these goals participants who are served within these programs are tracked across multiple waves of annual data collections.

PII is necessary in order to enable reliable tracking of students across multiple waves of these annual data collections. In addition, PII is necessary to verify that student records can be reliably connected for the same individual across these waves. Without PII, the Department would only have access to cross-sectional data that provides an opportunity to observe participations and program services in connection with one-year time horizon academic outcomes. With PII, the Department converts this cross-sectional data into a longitudinal format that allows for the observation of participation and services received over-time in connection with long-term academic outcomes.

This longitudinal view of the data allows the Department to perform required administrative functions, such as measuring grant project (and grant program) performance against established targets, which informs both grant monitoring and grant award making functions. It also enables the Department to perform research functions, such as evaluation of programmatic service components, the production and publication of program Fast Facts Reports, the production and publication of special topics research reports, and the generation of ad-hoc tabulations of respond to special data requests (such as those that emerge from Congress).

**1.3.** Is this a new system, or one that is currently in operation?

Currently Operating System

**1.4.** Is this PIA new, or is it updating a previous version?

Updated PIA

The PIA is being updated as part of the required biennial review.

**1.5.** Is the system operated by the agency or by a contractor?

Contractor

**1.5.1.** If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

## 2. Legal Authorities and Other Requirements

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

**2.1.** What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

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 PII in the TRIO programs cited in question 1.1.

**2.2.** Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

**2.2.1.** If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[5] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The SORN, titled "TRIO Programs Annual Performance Report (APR) System (TRIO APR)," 18-12-07, 74 FR 4168, was published in the Federal Register on January 23, 2009.

**2.2.2.** If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

**Records Management**

[5] 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

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

**2.3.** What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

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 DAA-0441-2013-0001.

**2.4.** Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

## 3. Characterization and Use of Information

### Collection

**3.1.** List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

PII is used to establish and maintain user accounts for federal employees and contractors, grantees in TRIO programs, and staff members at institutions. The PII elements collected are: first name, last name, email address, office phone number (optional), and cell phone number (optional).

The system collects work contact information about grantee project directors, certifying officials, and additional contacts. The PII elements collected are: first name, last name, email address, office mailing address, and office phone number.

The system also collects participant (i.e., student) information. The PII elements collected are: first name, last name, date of birth, race, gender, family income, family educational level, and educational information (e.g., grade point average, degree attainment, enrollment dates).

**3.2.** Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

**3.3.** What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The system collects information from Federal employees, contractors, grantee project directors, certifying officials, and additional contacts to establish and maintain user accounts.

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

**3.4.** How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The information is collected online, via a web application, and stored in a backend database.

**3.5.** How is the PII validated or confirmed to ensure the integrity of the information collected?[6] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

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.

Months before an annual data collection commences, the prior year student record file (i.e., the data matrix containing records of students served in the prior year's data collection) is extracted from the system. These records are matched within a longitudinal student record file which is maintained outside of the collection system, on an internal SharePoint site. Record matching occurs when six fields of information within the longitudinal student record file have identical information with records within the most recent APR collection. These fields include (1) the "PR" number (the unique identifier) for the grant project that served the student, (2) the student case number (the unique identifier for the student served), (3) the student's first name, (4) the student's last name, (5) the student's date of birth, and (6) any student cohort identifiers. If a match on all six

[6] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

fields is imperfect, then record matching is resolved manually. Once the matching is omplete, records are then uploaded back into the TRIO APR system.

**Use**

**3.6.** Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

PII is necessary in order to enable reliable tracking of students across multiple waves of these annual data collections. In addition, PII is necessary to verify that student records can be reliably connected for the same individual across these waves. Without PII, the Department would only have access to cross-sectional data that provides an opportunity to observe participations and program services in connection with one-year time horizon academic outcomes. With PII, the Department converts this cross-sectional data into a longitudinal format that allows for the observation of participation and services received over-time in connection with long-term academic outcomes.

This longitudinal view of the data allows the Department to perform required administrative functions, such as measuring grant project (and grant program) performance against established targets, which informs both grant monitoring and grant award making functions. It also enables the Department to perform research functions, such as evaluation of programmatic service components, the production and publication of program Fast Facts Reports, the production and publication of special topics research reports, and the generation of ad-hoc tabulations of respond to special data requests (such as those that emerge from Congress).

**3.7.** Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

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

☑ N/A

**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.*

**3.8.** Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

**3.8.1.** If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

**3.8.2.** Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

## 4. Notice

**4.1.** How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A Privacy Act Statement is included both on the opening page of the web application through which grant projects submit their APR data, and on the instructions document that the Department posts on-line to support the data collection.

**4.2.** Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

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 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. Providing the information on this form is voluntary; failure to disclose personal information 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.** What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, 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 project, 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.

**4.4.** Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

## 5. Information Sharing and Disclosures

### Internal

**5.1.** Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

**5.2.** What PII will be shared and with whom?

☐ N/A

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 UB and UBMS, TRIO submits APR data to the FSA, using secure transmission, so that the data can be matched to the NSLDS, providing TRIO with additional information on the extent to which UB and UBMS participants have enrolled in postsecondary education.

**5.3.** What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

This matching allows for a longitudinal view of the data to perform required administrative functions, such as measuring grant project (and grant program) performance against established targets, which informs both grant monitoring and grant award making functions. It also enables the Department to perform research functions, such as evaluation of programmatic service components, the production and publication of program Fast Facts Reports, and the production and publication of special topics research reports.

**External**

**5.4.** Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

No

**5.5.** What PII will be shared and with whom? List programmatic disclosures only.[7]
**Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.

☑ N/A

**5.6.** What is the purpose for sharing the PII with the specified external entities?

☑ N/A

**5.7.** Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

**5.8.** Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

[7] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

**5.9.** How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☑ N/A

**5.10.** Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

**5.11.** Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

## 6. Redress

**6.1.** What are the procedures that allow individuals to access their own information?

Individuals who wish to gain access to their own information must contact the system manager, and provide full name, address, telephone number and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. Requests must meet the requirements of the regulations in 34 CFR 5b.5 including proof of identity.

**6.2.** What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals who seek to contest the content of a record about themselves in the system must contact the system manager and provide identifying information including full name, address, and telephone number and any other identifying information requested by the Department while processing the request. The Department may request additional information to distinguish between individuals with the same name. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

**6.3.** How does the project notify individuals about the procedures for correcting their information?

The SORN listed in question 2.2.1 and this PIA explain the procedures for correcting information.

## 7. Safeguards

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

**7.1.** Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

**7.2.** Is an Authority to Operate (ATO) required?

Yes

**7.3.** Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

**7.4.** What administrative, technical, and physical safeguards are in place to protect the information?

TRIO APR is hosted outside of the Department's network on a FedRAMP-certified Amazon Web Services (AWS) GovCloud Cloud Service Provider (CSP). AWS enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards. Authentication to the server is permitted only over secure, encrypted connections.

TRIO APR has an ATO in place and is in compliance with all NIST standards related to security and encrypted connections. A firewall is in place which allows only specific trusted connections to access the data.

All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. In addition to the enforcement of the two-factor authentication and complex password policy, users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

**7.5.** Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

**7.6.** Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

**7.7.** Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The following tasks are performed to safeguard TRIO APR information:

- Annual contingency plan test performed.
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team.
- Annual updates to system security documents.
- Quarterly mandatory Cybersecurity and Privacy Training for employees and contractors.
- Monthly continuous monitoring is in place to include vulnerability scans, hardware/software inventories, and configuration management database updates are assessed and reported.

## 8. Auditing and Accountability

**8.1.** How does the system owner assess and ensure that the PII 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.** Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

**8.3.** What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with TRIO APR include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include embarrassment. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.