Privacy Impact Assessment (PIA)

for the

ED*Facts*

April 3, 2024

Point of Contact

Contact Person: Barbara Timm
Title: System Owner
Email: barbara.timm@ed.gov

System Owner

Name: Barbara Timm
Title: System Owner
Principal Office: Institute of Education Sciences

Submit completed Privacy Impact Assessments to the Privacy Office at
privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

ED*Facts* is a U.S. Department of Education (Department) initiative to collect, analyze, and promote the use of high-quality, pre-kindergarten through grade 12 data. This is done to:

- Support Department planning, policymaking, and management/budget decision-making.
- Centralize data provided by State education agencies (SEAs).
- Collect data on district and school demographics, program participation, and performance data.

ED*Facts* centralizes performance data supplied by SEAs within the Department to enable better analysis and use in policy development, planning, and management. The data collected are required to be submitted to the Department as conditions of grants that the Department provides to the SEAs.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

The ED*Facts* IT system is used to collect and process aggregated data on elementary and secondary education from States for several purposes, including grant management, public reporting, research, and compliance. All data collected are collected electronically through files and/or webpages.

The system collects contact information from State users and Federal employees to establish access credentials and maintain audit trails. For school years prior to 2022-23, the system collected contact information for the Chief State School Officers (CSSOs) to schedule site visits if necessary. CSSOs are the elected or appointed leaders of SEAs. The SEAs submitted the contact information for CSSOs through a file upload section of

the ED*Facts* system. While this information is no longer being collected, information previously collected on CSSOs is still present in the system.

Each State has one or more individuals who have access to ED*Facts* to submit data on behalf of the SEA. To set up system accounts, ED*Facts* collects these users' name, phone number, and email address.

Reports of student data are submitted by SEAs in an aggregate form; no personally identifiable information about students is provided in the SEA reports. The student data collected are counts that include statistics and demographic information at the local and individual school level, including the number of students enrolled by grade level, sex, race, ethnicity (data that conform to the Department's Final Guidance on Racial and Ethnic Data), and number of students participating in Elementary and Secondary Education Act Title I (Title I) programs.

Program office data stewards, including those representing the Institute of Education Sciences (IES), Office of Elementary and Secondary Education (OESE), and Office of Special Education Programs (OSEP), manage any publication of the data on the Department's public-facing website.

ED*Facts* uses an application called the SAS Business Intelligent tool for reviewing and analyzing data. ED*Facts* provides access to this tool to divisions in the Office of Finance and Operations (OFO). Those divisions use the tool to analyze and report on internal operational data from the Education's Central Automated Processing System (EDCAPS) and other sources as determined by OFO. Data analyzed through this method are generally used to create reports on the risk of grantees before grants are awarded, identify improper payments, and run reports for high-risk and at-risk grantees.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT

[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. OMB Circular A-130, page 33

system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

PII is obtained to provide access credentials to the ED*Facts* system, to facilitate communication between ED*Facts* personnel and users, and to maintain audit trails. The system collects contact information from State users and Federal employees to establish access credentials and maintain audit trails. For school years prior to 2022-23, the system collected contact information for the CSSOs to schedule site visits if necessary. CSSOs are the elected or appointed leaders of SEAs. The SEAs submitted the contact information for CSSOs through a file upload section of the ED*Facts* system. While this information is no longer being collected, information previously collected on CSSOs is still present in the system. For State users, ED*Facts* collects name, phone number, and email address to set up accounts in the system. The system collects and maintains usernames and passwords for these users. For CSSOs, EDFacts maintains name, work phone number, and work email address.

Separate from ED*Facts* operations, some divisions in OFO use the ED*Facts* SAS application to access data from EDCAPS as determined by OFO. The data accessed include the contact information of the representatives for grants, including name, job title, phone number, and email address. These data are not collected by ED*Facts*; they are collected through EDCAPS. The SAS application which is part of the ED*Facts* system is used to access these data for analysis and reporting by these divisions in OFO.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

The contractor's role is to develop and implement system changes, oversee operations, and provide system maintenance as needed, including but not limited to any other changes or updates as described in the contract.

☐ N/A

1.7. If the IT system is operated by a contractor, does the contract and other acquisition-related documents include privacy requirements?

Yes

☐ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The legal authority that permits the use of ED*Facts* is:

- Section 454 of the General Education Provisions Act, 20 U.S.C. 1234c.
- 34 CFR § 76.720 - State reporting requirements.

Under section (c) (1) - A State must submit these reports in the manner prescribed by the Secretary, including submitting any of these reports electronically and at the quality level specified in the data collection instrument.

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☐ Yes

☒ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

Records Management

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☐ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

☒ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

IES is waiting for the 21st Century Information Retention Policy Framework to be approved and implemented. In that Framework, ED*Facts* would fall under DAA-0441-2021-0002-0003 II.A. Completed Research and Statistical Studies.

Until that framework is implemented, the records will not be destroyed until the U.S. National Archives and Records Administration approves said schedule.

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

☐ Yes
☒ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☐ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☐ Home Address
☐ Personal Phone Number	☒ Work Phone Number	☐ Personal Email Address
☒ Work Email Address	☐ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☐ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☐ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☐ IP Address

☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☐ Other (Specify below)

If you have been directed to "specify below," describe the PII:

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:

Names are collected to maintain audit trails for the system.

☒ Federal Contractors

Specify types of information collected from Federal contractors:

Names are collected to maintain audit trails for the system.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[2]

CSSOs: prior to the 2022-23 school year, ED*Facts* obtained CSSOs' names, work phone numbers, and work email addresses.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

For State users, ED*Facts* collects name, phone number, and email address to set up accounts in the system. The system maintains usernames and passwords for these users.

Separate from ED*Facts* operations, some divisions in OFO use the ED*Facts* SAS application to access data from EDCAPS as determined by OFO. The data accessed include the contact information of the representatives for grants, including name, job title, phone number, and email address. These data are not collected by ED*Facts*; they are collected through EDCAPS. The SAS application which is part of the ED*Facts* system is used to access these data for analysis and reporting by these divisions in OFO.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

PII is collected from Department employees, contractors, and State representatives.

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

Individual users email ED*Facts* Partner Support to acquire access credentials for the system. Data accessed by OFO representatives via ED*Facts* is collected through EDCAPS.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

Name, work email, and work phone number are required to be submitted as part of the user account registration process and to validate that the user requesting access is authorized to register for the system.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒General Public (Any individual not employed by the Department)

State users only have access to data submitted by their State.

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

Annually, the ED*Facts* Partner Support sends the list of each State's users to each State's ED*Facts* coordinator who confirms that the individuals listed are authorized individuals in the State who should have accounts. At any time, the State ED*Facts* coordinator and the authorized individuals in the State can correct the information on individuals from the State who have accounts.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

No

3.9.1. If the above answer to question 3.10 is **YES**, cite the authority for collecting or maintaining the SSNs.

☑ N/A

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☑ N/A

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☑ N/A

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☑ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

The ED*Facts* website contains a privacy notice as a link from the ED*Facts* home page.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

☑ N/A

Click here to select.

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

Authorities: The following authorities authorize the collection of this information: 34 CFR § 76.720 - State reporting requirements. Under that section at (c) (1) a State must submit reports required under 2 CFR 200.327 (Financial reporting) and 2 CFR 200.328 (Monitoring and reporting program performance), and other reports required by the Secretary and approved by the Office of Management and Budget (OMB) under the

Paperwork Reduction Act of 1995, 44 U.S.C. 3501-3520 in the manner prescribed by the Secretary, including submitting any of these reports electronically and at the quality level specified in the data collection instrument.

Information Collected: For State users, ED*Facts* will collect the name, work phone number, and work email address in order to set up an account for that person in the system. The system collects and maintains usernames and passwords for these users.

Purpose: The purpose of collecting this information is to establish access credentials and maintain audit trails for State users and distribute information.

Disclosures: While information on State users will generally not be disclosed outside of the Institute of Education Sciences (IES), there may be circumstances where information may be shared with a third party, such as a Freedom of Information Act request, court orders or subpoena, or if a breach or security incident occurs affecting the system.

Consequences of Failure to Provide Information: Individuals representing the States are required to provide the information identified above to attain an ED*Facts* account. Failure to do so may result in not receiving an account.

Additional information about this system can be found in the Privacy Impact Assessment.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Individuals representing the States are required to provide the information identified above to attain an ED*Facts* account. Failure to do so may result in not receiving an account.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

No

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☑ N/A

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☑ N/A

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

No

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☑ N/A

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☑ N/A

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☑ N/A

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☑ N/A

Click here to select.

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Click here to select.

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☑ N/A

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☑ N/A

Click here to select.

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Individuals can change or delete their information by contacting the ED*Facts* Partner Support. Contact information for the Partner Support Center is provided on the ED*Facts* website. Users cannot see their information on the system, but they can see the information submitted in the email they send to register for access.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

Individuals can change or delete their information by contacting ED*Facts* Partner Support via email or telephone.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

All individuals with access to ED*Facts* receive a bi-weekly newsletter via email. ED*Facts* includes periodic notices in that bi-weekly newsletter about how to correct their contact information. Individuals are also notified in this PIA.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐ Low
☒ Moderate
☐ High

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

Access to the system is limited to authorized program personnel and contractors responsible for administering the ED*Facts* program or working on OFO analysis. Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing the ED*Facts* program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), ED*Facts* must receive a signed ATO in order to be operational. FISMA controls implemented by ED*Facts* are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and

accept a Rules of Behavior, and are required to utilize a complex password and two-factor authentication. The system is located in a protected environment. All sensitive data are encrypted in transit and at rest and access to records is strictly limited to those staff members trained in accordance with the Privacy Act of 1974, as amended.

8. Auditing and Accountability

8.1. How does the ISO assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the ED*Facts* system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and performs a weekly change management meeting that addresses all proposed and upcoming changes to its applications. The system owner also participates in the Department Change Management Change Advisory Board (CAB) meeting, to address proposed changes to the system and assess any potential new risk. The system owner also continuously monitors privacy controls to ensure effective implementation.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Continuous Diagnostics and Mitigation (CDM) scans are produced every week to identify security and privacy vulnerabilities which are reviewed by the system owner and ISSO. In the review, system owners are notified of any findings that require action. ED*Facts* also participates in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provides quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. ED*Facts* has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner, in coordination with the ISSO and the Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. ED*Facts* will also participate in quarterly and annual assessments and audits as required, including review of user accounts, to ensure the effective safeguarding of PII.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

Privacy risks associated with ED*Facts* include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII, and credentials are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. 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, utilizing least privilege principles, encrypting data in transmission, 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 regularly updating security patches and device operating 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.