Privacy Impact Assessment (PIA)

for the

ED*Facts*

January 27, 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: Barbara J. Timm / System Owner
Contact Email: Barbara.timm@ed.gov

System Owner

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

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.

ED*Facts* collects aggregate data on elementary and secondary education from the States for many purposes, including grant management, research, and compliance. The student data collected are counts that include statistics and demographic information at the local and individual school level, including number of students enrolled by grade level, sex, racial ethnic (data that conforms to the U.S. Department of Education's (Department) Final Guidance on Racial and Ethnic Data), and number of students participating in Elementary and Secondary Education Act Title I (Title I) programs. The system also contains descriptors of the schools (regular, vocational, etc.) and local education agencies (LEAs) (regular, special services, etc.). The data collected are required to be submitted to the Department through grants that the Department provides to the States. All data are collected electronically through file transfers and/or webpages via an approved information collection request. No personally identifiable information on individuals are collected. As with all aggregate data collection, there is a risk of the re-identification of individuals in circumstances with limited cell sizes. However, the ED*Facts* program has a policy to address and mitigate those risks to prevent re-identification, in collaboration with the Department's Student Privacy Policy Office.

The system collects contact information from State users and Federal employees to establish access credentials and maintain audit trails, as well as contact information regarding Chief State School officers (CSSOs) to schedule site visits if necessary. CSSOs are the elected or appointed leaders of State education agencies (SEAs). The SEAs submit the contact information for CSSOs through a file upload section of the ED*Facts* system.

Each State has one or more individuals who have access to ED*Facts* to submit data on behalf of the SEA. In order to set up system accounts for these users to submit data on behalf of their State, ED*Facts* collects these users' name and work contact information (phone numbers and email addresses).

ED*Facts* collects and processes the data. Program office data stewards, including those representing 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.

In addition, ED*Facts* provides access to the SAS Business Intelligent 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.

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

Information about CSSOs has been collected from the States to maintain contact information for scheduling site visits with State officials. Individual user information 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.

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?

New PIA

New guidance on how to apply the definition of PII required that a PIA be completed for the system. ED*Facts* collects and maintains the names and work contact information (address, phone number and email address) of CSSOs. CSSOs set up user accounts in order to submit their ED*Facts* data to the Department.

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

[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

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 that permits the use of ED*Facts* is: 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.

SORN

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?

No

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)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

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

Information is not retrieved by name or other personal identifier.

Records Management

[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

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.

IES is waiting on 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 such time as NARA approves said schedule.

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

No

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.

For CSSOs, ED*Facts* collects name, work phone number, and work email address.

For State users, ED*Facts* collects 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.

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

For Federal employees who access the ED*Facts* system, names are collected to maintain audit trails for the system.

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

Yes

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.

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

State agencies (for CSSOs) and individual users of the system.

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

Individual users email ED*Facts* to acquire access credentials for the system. Information regarding CSSOs are uploaded through file submission on the ED*Facts* website. Some of the data accessed via ED*Facts* is collected through EDCAPS.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Annually, the ED*Facts* Partner Support sends the list of each State's users to each State 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.

Use

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

User contact information (name and work email) is used to establish a user account on the ED*Facts* system so that the individual can complete required activities on behalf of their State agency. User information (name, work email, and work telephone number) is also added to the distribution lists by State so that the ED*Facts* partner support center

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

can distribute information to the user. CSSO information is collected to provide contact information for site visits to States.

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.

The ED*Facts* website contains a privacy notice as a link from the ED*Facts* home page. The privacy notice language is located in section 4.2.

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

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: 1) For Chief State School Officers (CSSOs), ED*Facts* collects name, work phone number, and work email address. 2) For State users, ED*Facts* collects 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, as well as obtain contact information regarding CSSOs to schedule site visits, if necessary. CSSOs are the elected or appointed leaders of State Education Agencies (SEAs). The SEAs submit the contact information for CSSOs through the file upload function of the ED*Facts* system.

Disclosures: The information on State users will not be disclosed outside of the Institute of Education Sciences (IES).

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.

4.3. 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?

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.

4.4. 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.

No

5.2. What PII will be shared and with whom?

☑ N/A

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

☑ N/A

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.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

[4] 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.

5.6. 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.

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

☑ N/A

Click here to enter text.

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 can change or delete their information by contacting 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 the subject individual to correct inaccurate or erroneous information?

Individuals can change or delete their information by contacting ED*Facts* partner support via email.

6.3. How does the project notify individuals about the procedures for 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.

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?

ED*Facts* resides on the Department's hosting platform (International Business Machines Corporation (IBM) Smart Cloud for Government (SCG)) and is required to follow all security measures and protocols defined by Office of Chief Information Officer (OCIO) Information Assurance Services (IAS).

- Access to ED*Facts* is only available to authenticated users who have a valid system user ID
- Management approves all access and roles and responsibilities.

- The logical boundaries of ED*Facts* are protected by a combination of firewalls, intrusion detection systems, and event monitoring systems.
- Every ED*Facts* user is provided a copy of the Rules of Behavior that they must acknowledge and sign prior to being granted access to the system.
- ED*Facts* servers are housed in environmentally controlled server rooms.
- There are scheduled system audits, user recertification/deprovisioning host and network intrusion detection, and vulnerability scans.
- Users outside the internal functional team and the individuals themselves have no access to PII.

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 ED*Facts* information:

- Monthly vulnerability scans performed
- Annual contingency plan test performed
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security AuthorizationTeam
- Annual updates to system security documents
- Annual mandatory Cybersecurity and Privacy Training for employeesand contractors
- Monthly Continuous Monitoring is in place with vulnerability scans (RA-05), hardware/software inventories (CM-08), and configuration management database updates (CM-06) are posted to CSAM.

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?

ED*Facts* performs a weekly change management meeting that addresses all proposed and upcoming changes to its applications. ED*Facts* also participates in the ED Change Management Change Advisory Board (CAB) Meeting. The system owner also continuously monitors privacy controls to ensure effective implementation.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

YesYes

8.3. What are the privacy risks associated with this 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 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. There are multiple layers of security and privacy protection in place to mitigate privacy risks of the ED*Facts* system. IES practices data minimization in order to collect the minimum amount of data necessary to perform the purposes specified in this PIA. ED*Facts* PII is limited to name, email address, and phone number of State CSSOs. This information is collected and stored in databases that are protected by multiple layers of security including firewalls and data encryption. This data are protected through encryption both in transit and at rest. While these protections and policies that apply to the system do not eliminate the risk of harm in the event of a breach, they do reduce to that risk to a level acceptable to the organization.