Privacy Impact Assessment (PIA)

for the

Education Stabilization Fund Public Transparency Portal (ESF PTP)

December 29, 2020

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: Keith Tucker
Contact Email: keith.tucker@ed.gov

System Owner

Name/Title: Gregory Fortelny, Chief Data Officer
Principal Office: OPEPD

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 Education Stabilization Fund Public Transparency Portal (ESF PTP) provides a public-facing website showing how grants authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act were allocated and what was done with the funds. The website includes a path to a data collection tool that is restricted to users authorized to submit annual performance report information for Education Stabilization Fund (ESF) grants. The system also feeds reports and dashboards for use by Department of Education (ED) staff.

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

Name and contact information for grantee points of contact is used for the purpose of coordinating the data collection. The PII is only used for creating user accounts for the grantee points of contact so they can submit the data collection responses, and for contacting the points of contact to resolve any issues with their responses. The names and contact information are not shared on the public-facing website.

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

New System

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

New PIA

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?

[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

☐ 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.

No specific reporting requirements for the ESF grants were cited in the CARES Act, so the general reporting requirements for ED grant programs are applied. The information collection is authorized under 20 U.S.C. 1221e-3, 1231a, and 3474, which allow the Secretary to promulgate rules and regulations to operate and govern ED's programs. The regulations authorizing the information collections conducted through the ESF PTP are defined in 34 CFR 75 and 34 CFR 76. Information collection instruments specific to reporting for the ESF grants were approved by the Office of Management and Budget in accordance with the Paperwork Reduction Act of 1995 and 2 CFR 200.327 and 2 CFR 200.328.

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

Click here to enter

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

[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 information managed by the system is not retrieved by an individual's name or personal identifier and is not maintained in a system of records.

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. 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.

ED 254, Grants Administration and Management Files – dispose 5 years after grant closure.
GRS 1.2, Grant and Cooperative Agreement Records - dispose 10 years after final action taken, unless further retention is required for business use

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.

This system collects and uses name, title (optional), office telephone number, and office email address of the points of contact for grant recipients under the CARES Act.

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

Yes

The system collects only the contact information for the grantees in order to coordinate the information collection, create user accounts, and contact the points of contact to resolve any issues with their responses. No information is collected that does not achieve this purpose.

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

The point of contact information already collected with the grant application is used to create accounts for submitting progress reports. ESF grantees may optionally provide information for additional points of contact to the ESF information collection help desk. In both situations, the information is collected directly from the ESF grantees, which are Institutions of Higher Education, State Educational Agencies, and State Governor's Offices.

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 PII already collected in the grant application is retrieved from the grants management system used to initially award the grants. Grant recipients may designate additional or alternative points of contact by providing their names and contact information to the ESF information collection help desk.

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?

The grantees' points of contact provide the PII directly. The email address provided is validated in the process of establishing a user account for the point of contact, and periodically checked for continued validity prior to annual reporting periods. Other contact information is validated only if needed to resolve issues with information collection responses.

Use

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

PII is used to establish user accounts for grantee representatives to use in submitting responses to an approved information collection. The email address is initially used to validate the account. The telephone number is used only if an information collection response contains errors that need to be discussed over the phone rather than through an email exchange.

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

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

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

Click here to enter

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

☑ N/A

Click here to enter

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.

This PIA is posted on the ed.gov notices page. A link to the posted PIA is included in the Terms of Use page presented upon logging in to information collection service, and in a verification email sent to points of contact during account creation.

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

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?

PII (name and email) associated with each ESF grant recipient is retrieved from the ED grants management system to create initial respondent accounts. Each respondent is contacted by email to verify accuracy of the email address and activate their account for submitting progress reports. After activating their accounts, individuals may voluntarily provide additional PII (phone number and title) as part of the information collection. Individuals may refrain from providing a telephone number or title and still be able to complete the information collection. Individuals may modify or deactivate their account

at any time by contacting the data collection help desk. Individuals may opt out by not activating their accounts.

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

Click here to enter

[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

Click here to enter

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

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 may view their account information by clicking the link to the account page in the data collection portal.

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

Individuals may modify or deactivate their account at any time by contacting the data collection help desk.

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

Users are advised of the procedure in the account creation process. A link to the account page is listed on the website for all users once logged in; the account page includes instructions on how to contact the help desk to correct user 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:

☐ N/A

Moderate

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

The Portal's internal network is protected from unauthorized access by firewalls. The network environment—including firewalls, servers, and desktops—are all protected from intrusions and viruses using the latest firewall and advanced malware mitigation solutions.

The system restricts the use of the data collection tool to authorized users with valid credentials and authority to complete the annual performance report on behalf of the grantee. Grantees are provisioned user accounts for submitting responses to the approved information collection using the web application dedicated to that purpose.

Access to the Portal web or database services are controlled using technical controls that ensure only authorized individuals can access the system. These services are scanned for

vulnerabilities and patched regularly to minimize the chance of a system/data compromise. All services are configured to forward logs to a centralized log repository that are monitored by security staff to identify misuse or threat actor attempts to compromise systems.

The Portal has technical and administrative controls in place that are compliant with the Federal Information Security Modernization Act (FISMA) and with National Institute of Standards and Technology (NIST) standards and guidelines. The system also operates under an approved Authorization to Operate.

The System Security Plan details the security and privacy requirements and describes the controls that are in place to meet those requirements.

The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a ‘‘need to know’’ basis and controls individual users' ability to access and alter records within the system.

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 system implements the Department's Risk Management Framework (RMF) processes and will be included in the Information System Continuous Monitoring (ISCM) program to minimize new threats or vulnerabilities. The continuous monitoring of security and privacy control effectiveness facilitates Ongoing Security Authorization (OSA) after the initial authorization is granted. The OSA program supports improved near real time risk reporting in accordance with updated NIST guidelines.

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?

The system owner reviews the website whenever functionality is changed to ensure the PII collection and usage practices are consistent with this PIA. The system owner also reviews weekly reports from the data collection help desk during annual data collection periods, which report any uses of the collected PII to contact grantee points of contact, in order to validate PII is used in accordance with the practices stated in this PIA. The system owner receives notifications of any information security incidents if they occur, and receives monthly reports of independent tests for vulnerabilities in the system's security protections.

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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

One privacy risk associated with this system is the potential for unauthorized access, use, or disclosure of PII pertaining to the users. These data breaches involving PII can be hazardous to individuals because they can result in identity theft or financial fraud. The risks are mitigated by the above-mentioned controls and safeguards, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.

Another privacy risk could entail human error related to database management. This risk is managed through the application of several controls identified in the system security plan (access controls, configuration management, audit and accounting, identification and authorization, boundary controls, etc.).

Additional privacy risks are mitigated as the system collects the minimum necessary PII to achieve the purpose. Additionally, the information collected is considered to be fairly low risk, as it is only name and work contact information and does not include any elements that have been identified as sensitive.