Privacy Impact Assessment (PIA)

for the

Education Stabilization Fund Public Transparency Portal (ESF PTP)

August 3, 2023

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/Deputy Chief Data Officer
Contact Email: Keith.Tucker@ed.gov

System Owner

Name/Title: Keith Tucker/Deputy Chief Data Officer
Principal Office: Office of Planning, Evaluation and Policy Development

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 (ESF) is a collection of grant funds appropriated in the Coronavirus Aid, Relief, and Economic Security (CARES) Act (Pub. L. 116–136) for use in responding to the novel coronavirus, COVID-19. ESF sub-funds initially consisted of the Elementary and Secondary School Emergency Relief (ESSER) Fund, the Governor's Emergency Education Relief (GEER) Fund, and the Higher Education Emergency Relief (HEER) Fund. Additional funds were appropriated for ESF through the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act (Pub. L. 116-260) and the American Rescue Plan (ARP) Act (Pub. L. 117–2), establishing an additional sub-fund named the Emergency Assistance to Non-Public Schools (EANS) Fund. The CARES, CRRSA, and ARP Acts defined funding amounts for each sub-fund and described permitted uses for the funds.

There are multiple programs for managing the ESF grants, corresponding to the sub-funds. The EANS, ESSER, and GEER sub-funds are managed by the U.S. Department of Education's (Department's) Office of Elementary and Secondary Education (OESE), and the HEER sub-fund is managed the Office of Postsecondary Education (OPE). Those offices manage applications for grants, allocation of formula grants, and monitoring of grant performance.

Public display of the grant allocation and use data on the ESF Public Transparency Portal (ESF PTP) at https://covid-relief-data.ed.gov is done in compliance with the Foundations for Evidence-Based Policymaking Act of 2018 (Pub. L. 115-435).

The ESF PTP provides a public-facing website showing how ESF grants were allocated to various state educational agencies (SEAs), Governor's offices, and institutions of higher education (IHEs), and what was done with the funds by the grantees. ESF PTP administrators extract financial transaction data, such as award amounts and withdrawals against those award amounts specific to ESF grants, from the USASpending.gov website, and combine it with data from other sources, such as the Common Core of Data (CCD) and the Integrated Postsecondary Education Data System (IPEDS), to show the financial data in context of States, SEAs, local education agencies (LEAs), and IHEs.

The public download tools for the various data sources are used to manually retrieve the latest data from each source, and then the data sets are combined programmatically using the common identifiers shared between them. For example, the USASpending data includes a Unique Entity Identifier (UEI) for each grantee, which is matched to the same identifier for SEAs in the CCD extract, and the IHEs in the IPEDS data extract.

To facilitate grant performance monitoring, ESF PTP also includes a data collection capability for grant recipients to submit annual performance reports (APR) describing in detail how funds were used and the planned uses for remaining funds. The APR data collected from individual grantees are used to generate internal reports that contain aggregated, summarized information from all the APRs. A privacy-protected derivation of the APR data is also displayed publicly on the ESF PTP website for accountability. This version removes narrative elements that are present in APRs and suppresses data values from small cell sizes to mitigate the possibility of reidentification of individuals.

The grant data is aggregated by State, with a further breakdown by IHE and LEA within a State. The ESF PTP website contains an interactive United States map, from which users can select a State to view data specific to grant allocations to organizations within that State. Users can also search by LEA or institution name to jump directly to the grant data for that organization.

Financial data from USASpending.gov, a public data source, are extracted by the ESF PTP administrators and combined with geographic and organizational data from other public sources, namely the Department's IPEDS, and CCD public data assets, and the Census Bureau's population data, to provide the grant performance transparency features. More information about the data used to produce the public-facing display is provided on the ESF PTP application website, at https://covid-relief-data.ed.gov/about-data.

Additional financial data, detailing subawards for the grant funds, expenditures of the grant funds, and planned uses of remaining funds, are collected in the APRs submitted through the ESF PTP. The APR data include summaries of how much funding was expended in each category of permitted use, funding allocations to LEAs within the corresponding State, the number and demographics of students impacted by the fund uses, and how many jobs, broken down by various categories, such as nurses, special educators, and school counselors, were created or retained through the use of grant funds.

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

Contact information for grantee points of contact is collected for the purpose of coordinating the submission of APRs. PII is 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 contact information is not shared on the public-facing website.

Information is also collected from system administrators for the purpose of creating user accounts to manage access to the system.

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 regular 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

[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 information collection is authorized under 20 U.S.C. § 1221e-3, 1231a, and 3474, which allow the Secretary of Education to promulgate rules and regulations to operate and govern the Department's programs. The regulations authorizing the information collections conducted through ESF PTP are defined in 34 CFR § 75 and 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 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

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

The information managed by the system is not retrieved by an individual's 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.

General Records Schedule 1.2, Grant and Cooperative Agreement Records, Item 020 – Destroy 10 years after final action is taken on the grant, but longer retention is authorized if 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.

From grantee points of contact: name, title, work email address, work phone number, username, and password.

From Department contractor system administrators: name, work email address, username, and password.

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

Yes

The system collects the minimum amount of information for the purposes of creating accounts to access the system to submit APRs and contact individuals, as needed, to resolve any issues with the APRs. No information is collected that is not needed to achieve this purpose.

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

ESF PTP system administrators use point of contact information retrieved from G5, the Department's grant management system, to create accounts for grantee representatives to submit progress reports. This is done through a manual retrieval. ESF grantees may optionally provide information for additional points of contact via email to the ESF help desk. In both situations, the information is initially collected directly from the ESF grantee points of contact.

PII for system administrators is collected directly from the individuals to establish their accounts.

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 is retrieved from the grants management system that is used to initially award the grants to establish initial accounts for each grantee. Grant recipients may designate additional or alternative points of contact by providing their names and contact information to the ESF help desk.

System administrators provide information for creating their accounts through web forms.

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 email address provided is validated in the process of establishing a user account for the point of contact by sending a confirmation link to the provided email address; the account is not activated unless the link is followed. Email addresses are checked for continued validity using email messages broadcast to all points of contact prior to and during annual reporting periods; accounts for which the email messages fail to deliver are deactivated.

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. PII is also used to establish user accounts for system administrators.

[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.

3.7. 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.

Department grant records originate in the G5 system, a component of Education's Central Automated Processing System (EDCAPS). EDCAPS is responsible for all grants' pre- and post-award processing, including grant payment processing. Point of contact information is retrieved from G5 manually to allow for the creation of user accounts for access to the ESF PTP. Notice is provided by the G5 system when a grant is

approved for an institution. For additional information related to the notice provided by the G5 system, please refer to the EDCAPS PIA, located on the Department PIA website. Once information is retrieved from G5, accounts for institutions are created by the ESF PTP administrator.

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

For additional information related to the notice provided by the G5 system, please refer to the EDCAPS PIA, located on the Department PIA website.

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?

Providing information to ESF PTP is voluntary. Institutions and individuals have the opportunity to decline to provide the information; however, providing certain information is required to create accounts for meeting reporting requirements necessary to receive grant funding. Individuals may modify or deactivate their account at any time by contacting the ESF PTP help desk.

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

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

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

[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.

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 a link to their account page in the ESF PTP.

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 ESF PTP help desk.

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

Users are advised of the procedure during 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 ETF PTP 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: **Low, Moderate, or High?**

☐ N/A

Moderate

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

The ESF PTP internal network is protected from unauthorized access by firewalls. The network environment, including firewalls, servers, and desktops, are protected from intrusions and viruses using the 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 ESF PTP 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 ESF PTP 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. ESF PTP 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 will be facilitated through the Ongoing Security Authorization (OSA) program. The OSA program supports improved 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?

Privacy risks associated with ESF PTP 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 or loss of credentials that are used to gain access to other resources. 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 and updating devices' operating software. 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.