Privacy Impact Assessment (PIA)

for the

Payment Integrity Monitoring Application (PIMA)

May 12, 2021

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: Diana Sanchez/Financial Management Analyst and ISO
Contact Email: Diana.sanchez@ed.gov

System Owner

Name/Title: Diana Sanchez/Financial Management Analyst and ISO
Principal Office: Office of Finance and Operations

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.

Payment Integrity Monitoring Application (PIMA) is an application that integrates payment analysis, case management, and reporting functions to automate and streamline the detection, recovery, and prevention of improper payments. PIMA is an application that runs on the ServiceNow platform. ServiceNow is a cloud service provider. The functionality of PIMA demonstrates compliance with the Payment Integrity Information Act of 2019 (PIIA) and Office of Management and Budget (OMB) Circular A-123, Appendix C.

The purpose of PIMA is to detect anomalies in grants payment data. Case management files for payment anomalies are established within the application for follow-up investigation by the U.S. Department of Education's (Department's) grants program officials to validate improper payments and determine root causes. Data analyzed through this method are used to identify improper payments.

PIMA gathers grant refund data, which contain the grantee award number, refund amount, and grantee contact information (only for institutions that have received grants). Grantee contact information is collected to facilitate further information gathering and determining root causes of grant refunds. PIMA also collects information from two distinct groups within the Department: program officers and program office points of contact (POCs). Of these two groups, only POCs have access to PIMA due to licensing limitations. This access is view-only; POCs cannot alter any information in the system. Grant refund data are sent to PIMA via email from SAS (SAS is statistical software suite managed by the EDFacts system). This process is fully automated; PIMA automatically pulls information from the emails with no required human interaction. POCs monitor grants on the PIMA system, emailing program officers when action is needed using the contact information collected in PIMA. Once the program officer receives the email from the POC, the program officer requests information from the grantee via email.

Some staff members of the Office of Financial Management (OFM) have access to PIMA for system administration. The system maintains their names, usernames, and passwords as access credentials. Access credentials are established when the user is first granted access to the system.

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

The program office points of contact (PIMA system users) use the personally identifiable information (PII) from the grant refund to reach out to the program officer within the Department responsible for overseeing that particular grant. The program officer receives information about the grant refund, which institution made the refund and the point of contact at the institution. This information is used to identify the individual at the institution who can provide the reason for the grant refund and potential improper payment root cause.

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

A review of this system identified a need to revise this PIA to accurately represent PII collected by the system.

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.

Payment Integrity Legislation
Payment Integrity and Information Act (PIIA) of 2019
United States Code (USC)
31 USC 3321: Disbursing authority in the executive branch
2 CFR § 200.53 (December 2014, "Uniform Guidance")
Presidential Actions
Executive Order 13520, Reducing Improper Payments (November 20, 2009)
OMB Circulars and Memoranda
M-21-19, Appendix C to Circular No. A-123, Requirements for Payment Integrity Improvement (Mar 5, 2021)
OMB Circular A-136, Financial Reporting Requirements (August 27, 2020)

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

2.2.3. 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 is not retrieved by an identifier. The information is retrieved by a SAS query from the Department's Grants Management System (G5) tables using the grant number for awards, refunds, and appropriations. As stated in the section 1.1, the process of determining refunds is automated and grantee POC information is not retrieved by a personal identifier but rather by grant number

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.

General Records Schedule (GRS) 1.2, item 020: Grant and cooperative agreement case files, successful applications.
Retention: Temporary. Destroy 10 years after final action is taken on file, 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.

All of the information in the system is collected from G5.

Point of Contact (POC) Information. The following is captured in PIMA to establish cases within the system and route cases to the correct personnel:

- Program office
- Program office POC name
- Program office POC email address
- Program office POC phone number

Program Officer Information. The following is captured for the use of the Program Office POC to reach out to the Program Officer:

- Program office
- Program officer name
- Program officer email address
- Program officer phone number

The following is captured for the use of the Program Officer to contact the grantee:

Institutions Only

- Grantee name (institution name)
- Grantee contact name (first and last)
- Grantee contact email address
- Grantee contact phone number
- Grantee contact address (street, city, state, zip)

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

Yes

Program office information and grantee information is collected to establish cases, contact program officers, and contact grantees. The system only collects the minimum necessary
information required to establish cases and identify and contact the points of contact.

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

PIMA pulls all of the information from G5. G5 collects the information from individuals and schools. Please see the PIA for EDCAPS for information about how G5 collects the information.

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

Collected from the Department's G5 database. Please see the PIA for EDCAPS for information about how G5 collects the information.

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 PII is validated as it is collected and maintained by the G5 system. PIMA pulls all of the information from G5.

Use

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

The PII is used to address payment integrity issues by contacting the individuals (grant program officers within the Department) involved in the questioned payment activity. When a payment integrity issue is identified by PIMA, a case is created and the PII is used to contact the individuals associated with the payment integrity issue in order to resolve the issue. The grant refund includes the name of the institution and a point of contact at the school.

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

Click here to enter text.

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.

[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.

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 text.

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 text.

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.

PIMA does not collect PII directly from individuals. PIMA pulls all of the PII from G5. Please see the PIA for EDCAPS for information about how G5 collects the information.

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

Click here to enter text.

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?

Opportunities to consent to uses are provided at the collection point in EDCAPS. Please see the PIA for EDCAPS for information about how G5 collects the information.

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

Yes

5. Information Sharing and Disclosures

Internal

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

Yes

5.2. What PII will be shared and with whom?

□ N/A

The Department program offices that receive grantee information are Institute of Education Services (IES), Office of Postsecondary Education (OPE), Office of Elementary and Secondary Education (OESE), Office of Career, Technical, and Adult Education (OCTAE), Office of Special Education and Rehabilitative Services (OSERS), and Office of English Language Acquisition (OELA). The program offices will receive the program officer name, telephone number, and email address. They will also receive the grantees (institutions only) point of contact, address, telephone number, and email address.

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

□ N/A

To assist with the investigations of improper payments.

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 text.

[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 text.

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?

The G5 system is the source of the data that feed into PIMA. Please see the PIA for EDCAPS for the procedures that individuals will need to take to access their own information.

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

The G5 system is the source of the data that feeds into PIMA. Please see the PIA for EDCAPS for the procedures that will allow the individual to correct inaccurate or erroneous information in the system.

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

The G5 system is the source of the data that feeds into PIMA. Please see the PIA for EDCAPS for how the project will notify individuals on the procedures for correcting their 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

Low

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

The protection of the information in PIMA is partially inherited from ServiceNow for physical security, which is approved for FedRAMP moderate and from the Department for network security. Safeguards are based on guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, and 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. Key safeguards include Access Controls, Awareness and Training, Audit and Accountability, Security Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Security Planning, Personnel Security, Risk Assessments, System and Communications Protection, System and Information Integrity, and System and Service Acquisition.

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 protection of the information is partially inherited from ServiceNow, which is approved for FedRAMP moderate, and Department network security. PIMA can only be accessed through the Department network, which requires a PIV card. Once on the Department network, PIMA is further protected by multi-factor authentication. The monitoring, testing, and evaluation of physical security is conducted by ServiceNow, and network security by the Department. PIMA undergoes annual system security authorization to maintain an active authorization to operate (ATO). The ATO process includes an assessment of security and privacy controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program. Web scans, database scans, and penetration testing are conducted on the system based on established system schedule for scanning as part of testing and monitoring of the system. There are also scheduled system audits, end-user recertification/deprovisioning, and vulnerability scans.

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 protection of the information is partially inherited from ServiceNow, which is approved for FedRAMP moderate. ServiceNow performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the ServiceNow Government Cloud components. If PII is discovered, a Privacy Impact Assessment is performed. In addition, the PIMA system owner conducts a Privacy Threshold Analysis and a Privacy Impact Assessment every two years.

The PIMA system owner ensures that the use of information follows stated practices in this PIA through several methods. One method is completing the Department's Risk Management Framework process and receiving an authorization to operate (ATO). Under this process, a variety of controls are assessed by an independent assessor to ensure the PIMA application and the data residing within are appropriately secured and protected. One third of all NIST security controls are tested each year, and the entire system's security is re-evaluated every three years. The PIA is reviewed and updated on an as-needed basis and, at a minimum, biennially. These methods ensure that the information is used within the stated practices outlined in this PIA.

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 to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. Additionally, privacy risks have been reduced by only collecting the minimum PII necessary and by not collecting any sensitive PII.

Access to monitoring and auditing related documents are limited to Department employees with appropriately approved access authorization.