Privacy Impact Assessment (PIA)

for the

Impact Aid Grant System

April 21, 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: Amanda Ognibene, Group Leader, Impact Aid Program
Contact Email: Amanda.Ognibene@ed.gov

System Owner

Name/Title: James Le, Information System Owner
Principal Office: Office of Elementary and Secondary Education (OESE)

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 U.S. Department of Education's (Department) Impact Aid Program (IAP) manages multiple formula grant award programs authorized by Title VII of the Elementary and Secondary Education Act. Impact Aid grants are awarded to local education agencies (LEAs) that experience a decrease in local tax revenue due to the presence of non-taxable Federal land. The Impact Aid grant applications are submitted by LEAs annually with statistical information about the size and location of Federal property and/or the number of children who either live on or whose parents work on Federal property. LEAs collect the information necessary to complete the application by doing an annual survey (either a parent-pupil and/or a source-check survey(s), described below) of its student members to determine which students live on Federal property and which students have parents who live or work on Federal property or are members of the uniformed services. The Impact Aid grant applications do not include any personally identifiable information about students or their parents. More information on the Impact Aid Program is available at https://impactaid.ed.gov.

The Impact Aid Grant System (IAGS) is the management and information system supporting the day-to-day processes of the IAP. It is used by Department staff, LEA staff, and State education agency (SEA) staff. LEAs submit the annual grant application and view payment vouchers in IAGS. Payment vouchers are reports that show the data used to calculate formula grant payments, the total amount of the payments, and the dates payments were processed. SEA users can view application and payment information for LEAs in their State. Department staff review and monitor each application. When Department staff are finished reviewing the data contained in an application, the system calculates a formula grant payment and communicates the amount of the payment to the applicant and to G5, the Department's main grant processing system where payments are processed. IAGS does not contain financial information about individuals.

On an annual basis, the Department will audit twenty (20) percent of applications received. These selections are based on a risk-based assessment that is conducted by the IAP. If the LEA(s) are audited, IAP requests all documentation that was used to

formulate calculations/counts that was submitted to the Department. The documents that the LEA provides may contain information about parents and students who live or work on Federal property or are members of the uniformed services. Most audits can take up to 6 months, but typically less than a year.

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

The data in the system are related to the annual Impact Aid grant applications submitted by LEAs, which are used to calculate formula grant payments. IAGS includes information about the size and type of eligible Federal property, counts of children either living on the property or whose parents work on the property, as well as statistical finance information such as the LEA's total current expenditures and the percentage of revenues it receives from local sources. The Impact Aid Program reviews the LEA's annual survey responses to ensure that the LEA filled out the application correctly. These survey responses may be part of the application file. These files are not searchable and contain information such as student names, parent names, home addresses, and information about parents' employment.

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 required 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

[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

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.

The program is authorized by Title VII of the Elementary and Secondary Education Act (ESEA), 34 CFR § 222, as amended. Title VII allows for the establishment and maintenance of the program, including determining LEA eligibility and auditing eligible LEAs.

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

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

[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

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.

The records retention schedule for IAGS is GRS 1.2: Grant and Cooperative Agreement Records. Records are destroyed 10 years after the last action is taken on the 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.

From Federal employees and contractors: name, work email address, and work phone number.

From LEA and SEA personnel: name, State, job title, phone number, and email address.

From students/parents:
The information listed below is collected through the parent-pupil survey by LEA personnel and provided to the Department with the application. When the Impact Aid Program audits/monitors a grant application, it requests survey documentation (either a parent-pupil and/or a source-check survey(s), described below) from the LEA. The documents that the LEA provides may contain information about parents and students who live or work on Federal property or are members of the uniformed services. The information required to be collected in the Impact Aid survey is outlined in 34 CFR 222.35.

Information collected in the parent-pupil survey includes:

- From students: name, date of birth, school name, grade level, and home address.
    - If the student's residence is on Federal property, the name of the Federal facility in which the student resides.
- From parents: name and signature.

- If a parent is employed on Federal property: name and address of the employer.
- If a parent is an active member of uniformed services: rank and branch of service.

If there is a group of students being claimed on the Impact Aid application by Federal property, information about the group of students is collected through the source-check survey. This survey is used in place of the parent-pupil survey form to substantiate a pupil's place of residence or parent's place of employment on the survey date. For example, a school district may provide a list of students that fall under the requirements of the IAP. A certifier (depends on the type of federal property, for example, base housing official) would then certify the information provided by the school district. Information collected through the survey contains the same PII elements as above, but also includes the following:

- Certification by a parent's employer regarding the parent's place of employment;
- Certification by a military or other Federal housing official as to the residence of each pupil claimed;
- Certification by a military personnel official regarding the military active duty status of the parent of each pupil claimed as active duty uniformed services; or
- Certification by the Bureau of Indian Affairs or authorized tribal official regarding the eligibility of Indian lands.

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

Yes

IAP collects only the minimum information necessary to administer the program. Contact information is needed to communicate with the SEA and LEA recipients and administer the program. Additional information, such as parent and student information is collected as part of an audit and is needed for auditing purposes. This information is needed to determine whether a child or their parent lives/works on Federal property. The IAP uses this information to cross-reference the student's address against Federal property records to ensure the student resides on, or the parent works on, Federal property. No information is collected that is not required to achieve these purposes.

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

The LEAs collect information from or about (if provided by a school district, for example) individual students and parents. The LEAs total the number of children for each property and/or category and submit the total numbers in the Impact Aid grant application through the IAGS. The statistical information submitted contains the high-level student count totals and not the PII of eligible students/parents living or working on Federal properties. Audit information is collected from LEAs and is provided to IAG. LEA and/or SEA personnel information is collected directly from the LEA or SEA.

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

LEAs provide their personnel information on applications submitted to the IAP. LEAs collect information from or about parents and students using parent-pupil and source-check surveys. When the Department conducts an audit and requests supporting documentation from the LEA, the LEA will provide the surveys used to collect the information and perform calculations to the Department in PDF format. The LEAs will upload the information via attachments to an application when the application is audited, as requested by IAP.

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?

For source-check surveys, student information is validated by the LEA, and employment and residence information is verified by a certifier with knowledge of the connection to Federal property (e.g., a Bureau of Indian Affairs or tribal official, a Federal Housing official, or a military base housing official). The certifier validates that this address reported is Federal property and certifies that the individuals are employees, contractors, residents, or otherwise connected to that property. In addition, if an LEA is audited by the Department, information is verified to ensure the initial submission of calculations provided by the LEA were correct.

Use

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

LEA personnel name and contact information are collected as part of the application process to provide points of contact to IAP. LEAs collect student and parent information on the annual Impact Aid application to count students who belong to families who live

[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.

on or work on Federal, tax-exempt properties. When the application is audited by IAP, IAP staff may request the LEA to upload student-level data to IAGS. IAP staff use the uploaded files to verify that the students were appropriately counted, verified, and categorized for payment.

SEA users can view application and payment information for LEAs in their State. SEA users request system access using a form on the IAGS website that requests their State, job title, email address, and phone number. IAP staff create an account for SEA users after confirming their contact information matches that given on the State's website. SEA users can view application and payment information for LEAs in their State.

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, or PIA,)? If notice is not provided, explain why not.

The IAP does not directly collect PII from parents and students; all individual-level information is collected by the LEAs, which maintain their forms for collection. The LEAs are responsible for providing notice to parents and students since they administer the forms by which information is collected. IAGS does not provide notice to parents and students about the collection of PII. State and local laws where the LEA is located apply to notices to individuals of their privacy rights.

This PIA provides notice on the uses of PII collected from LEAs concerning the IAP.

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?

Because LEAs collect the information using their survey processes, each LEA determines the opportunities for individuals to provide consent.

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?

No

The IAP does not directly collect PII from parents and students; all individual-level information is collected by the LEAs, which maintain their forms for collection. The LEAs are responsible for reviewing and updating their notices accordingly.

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

What PII will be shared and with whom?

☐ N/A

PII is shared with the Department's G5 system, which administers grant awards from planning through closeout, including disbursing funds to grant recipients for certain Department programs. To learn more about the G5 system, please refer to the "Education's Central Automated Processing System (EDCAPS)" PIA, located on the Department's public-facing PIA website.

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

☐ N/A

When Department staff are finished reviewing the data contained in an application, the system calculates a formula grant payment and communicates the amount of the payment to the applicant and G5. G5 is responsible for the disbursement of the payment to the recipient.

External

5.2. 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

5.3. 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

5.4. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

5.5. Is the sharing with the external entities authorized?

☑ 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.

5.6. 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.

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

☑ N/A

5.8. 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.

5.9. 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 Department does not collect PII directly from individuals. Information is collected by LEAs directly from individuals. Individuals must contact LEAs to access their information.

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

The Department does not collect PII directly from individuals. Information is collected by LEAs directly from individuals. Individuals must contact LEAs to access and correct their information.

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

The LEAs are responsible for notifying individuals about 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

Moderate

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

IAGS is hosted on the FedRAMP-certified Amazon Web Services (AWS) GovCloud Cloud Service Provider (CSP). AWS enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards. Authentication to the server is permitted only over secure, encrypted connections.

IAGS has an ATO in place and complies with all National Institute of Standards and Technologies (NIST) standards related to security and encrypted connections. A firewall is in place which allows only specific trusted connections to access the data.

IAGS is only accessible to authorized users. User access is managed by IAP. IAGS supports secure communication protocols for IAGS users and systems connected to IAGS, such as G5, which is used to process payments for LEAs. All personnel working with IAGS must agree to established rules of behavior. Personnel in system administration and support roles must complete personnel background screening for moderate risk and complete additional training including role-based, incident response, and disaster recovery training.

Data are maintained in a secure data center, access to which is governed by multiple access controls. IAGS technical and administrative controls comply with the Federal Information Security Modernization Act (FISMA) and with NIST standards. IAGS uses a FedRAMP-approved cloud service provider; third-party assessment organizations are responsible for periodically verifying the technical and physical safeguards.

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 IAGS information:

- Annual contingency plan test performed.
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security Authorization Team.
- Annual updates to system security documents.
- Quarterly mandatory Cybersecurity and Privacy Training for employees and contractors.
- Monthly continuous monitoring is in place to include vulnerability scans, hardware/software inventories, and configuration management database updates are assessed and reported.

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 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 system owner makes sure that

the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of 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 and meets regularly with the information system security officer.

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 IAGS 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. 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 per the patch scheduling and updating devices operating software, amongst other 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.