Privacy Impact Assessment (PIA)

for the

Impact Aid Grant System

October 1, 2020

For PIA Certification Updates Only: This PIA was reviewed on **October 1, 2020** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Amanda Ognibene / Senior Analyst
Amanda.Ognibene@ed.gov

System Owner

Name/Title: Kristen Walls
Principal Office: Office of Elementary & 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 Impact Aid Program (IAP) is a Federal formula grant program administered by the U.S. Department of Education (DoED) Office of Elementary and Secondary Education (OESE). It is designed to ease the financial burden placed on resources of local educational agencies (LEAs) due to certain activities of the Federal Government. Because local schools usually are supported by local real property taxes collected from property owners in the geographic area of the LEA, the ownership of property by the Federal Government reduces the amount of available local tax revenue and may increase the number of children enrolled in the LEA. Impact Aid payments provide the financial assistance to certain LEAs impacted by this financial burden.

The Impact Aid Grant System (IAGS) will provide a public application interface to allow full grants life-cycle management, including: application submission, application review, grant award approval, payment calculation, financial reporting, grantee communications, issue management, and workflows. Data collection will occur during the grant application process and during the application review and audit processes.

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

LEAs submit source forms on which initial eligibility determinations for LEAs are made and as part of the grantee audit process. Name and work contact information of LEA personnel are collected to administer the program and to contact the LEA if needed.

IAP uses a risk-based audit selection process that results in grantees being audited, on average, once every five years. In the event of an audit, the documents submitted to auditors may include the following information from parents and students who live or work on Federal property, or who are members of the uniformed services:

- Name and date of birth of student
- Name and home address of parent
- Parent’s rank and branch of service if on active duty

[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

- Parent’s employer address, if located on Federal property

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

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

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), as amended. The program regulations are in the U.S. Code of Federal Regulations at 34 CFR 222. Allow for the establishment and maintenance of the program, including determining LEA eligibility and for 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

Click here to enter text.

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 using an individual name or other 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

2.3. 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.

Yes. The ED records schedule is 254: Grants Administration and Management Files (N1-441-11-001). Records are destroyed 10 years after 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.

[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

LEA Personnel: Name, phone number, and email address.

In the event of an audit of a grantee, the documents provided and maintained in the system may also include the following information from parents and students who live or work on federal property, or who are members of the uniformed services:

- Name and date of birth of student
- Name and home address of parent
- Parent’s rank and branch of service if on active duty
- Parent’s employer address, if located on Federal property

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 LEA recipients and administer the program. Additional information, such 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 individual students and parents. The LEAs total the number of children for each property and/category and submits the total numbers in 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. LEA personnel information is collected directly from the LEA. Audit information is collected by from parents and students by LEAs and is provided to IAG.

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 parents and students using Parent-Pupil Surveys and the Source Check Form. These paper forms are combined via PDFs. The LEAs will upload the information 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?

In the case of Parent-Pupil survey forms, information is validated by the student's parent. In the case of a Source Check form, student information is validated by the LEA and employment/residence information is verified by a certifier with knowledge of the Federal connection (for example, a Bureau of Indian Affairs or tribal official, a Federal Housing official, or a military base housing official).

The certifier validates that the address reported is Federal property and certifies that the individuals reported by the LEA are in fact employees/contractors/residents or otherwise connected to that property.

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 so IAP has a point of contact.

Applicant LEAs collect student and parent information in order to count students who are federally connected on the annual Impact Aid application. Federally connected students are students who belong to families who live on or work on Federal, tax-exempt properties. When the application is audited, IAP staff may request for 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.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

[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.

3.7.1. 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.

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.

IAP collects LEA personnel information as part of the application process.

IAP does not directly collect PII from parents and students. As a result, IAGS does not provide notice to individuals about the collection of PII because Impact Aid grants are awarded to LEAs, not individuals. The LEAs collect and maintain individual forms from parents and students. State and local laws where the LEA is located apply with regard to notices to individuals of their privacy rights.

This PIA will be posted to the ed.gov/notices webpage.

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?

The LEA personnel information is provided by the personnel only for contact purposes. LEAs choose to provide this information, but no consent is obtained.

LEAs collect the information from individuals who agree to its stated uses. Individuals may decline to provide information or opt-out without penalty.

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

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

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

[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?

LEA personnel must work with IAP to access their information.

Individuals must work with the LEA to access their own information. IAGS does not store information for retrieval by individual identifiers.

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

LEA personnel may contact IAP to correct their information.

The individual must request contact the LEA for information correction. The LEA must verify the accuracy of the corrected information before submitting the correction to IAGS.

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

LEA personnel submit the applications, and if they wish to update the point of contact, they reach out to the IAP.

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 access is only available to authorized users. User access is managed by IAP and the LEA. IAGS only supports secure communication protocols for both IAGS users and DoED interconnected systems. All personnel working with IAGS have to agree to established rules of behavior. Personnel in system administration and support roles must successfully complete personnel background screening for moderate risk and complete additional training including role-based, incident response, and disaster recovery training.

Physical security of electronic data will be maintained in a secured data center, access to which is controlled by multiple access controls. IAGS technical and administrative controls are in compliance with the Federal Information Security Management Act (FISMA) and with National Institute of Standards and Technology (NIST) standards. IAGS utilizes a cloud service provider registered with General Services Administration's (GSA) Federal Risk and Authorization Management Program (FedRAMP) where independent third-party assessment organizations(3PAOs) are responsible for verifying technical and physical safeguards periodically.

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.

IAGS will be authorized for operation in accordance with the Department's Security Authorization Program. As part of the Authority to Operate (ATO) granted by the Security Authorization Program, IAGS will be required to comply with both the current version of NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and organizations and the Department's Information Security Continuous Monitoring Roadmap. Examples of testing or evaluation include running vulnerability scan and mitigating vulnerabilities within the times specified by the Department in addition to performing yearly self-assessments on one-third of the applicable security controls.

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 IAGS system owner ensures that the information is used in accordance with stated practices in this PIA through several methods. One method is completing the ED Risk Management Framework process and receiving an Authority to Operate (ATO). Under this process a variety of controls are assessed by an independent assessor to ensure the IAGS application and the data residing within are appropriately secured and protected. One-third of all controls are tested each year and the entire system security is reevaluated every three years. The PIA is reviewed and updated on an as needed basis and at a minimum, annually. In addition, the OMB authorizations are reviewed and updated on a federally mandated schedule. These methods together with regular communication with the IAGS users ensures 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 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.

Additionally, privacy risks have been reduced by not requiring or requesting Social Security Numbers (SSN) for the grant’s application process. In the event that SSN or PII is inadvertently submitted by grant applicants, the system encrypts data at rest and in transit to protect from unauthorized disclosure. Role-based access controls are implemented to ensure access to data are restricted to authorized users only. System logs record attempted unauthorized access to stored information. Additionally, PII data, when required for grant monitoring and audit purposes, is requested, uploaded, accessed, and stored separately from the grant application documents. Access to monitoring and auditing related documents are limited to Department of Education employees with appropriately approved access authorization. PII data will not be posted to the IAGS Public Portal for any reason.