



**Privacy Impact Assessment (PIA)**  
for the

Integrated Student Experience(ISE) StudentAid.gov

Nov 19, 2018

This PIA was originally approved on Apr 4, 2014 and reviewed on Nov 19, 2018 by the system owner certifying the information contained here is current and up to date.

**Contact Point**

**Contact Person/Title:** Jessica Barrett Simpson/Supervisory Borrower Experience Specialist

**Contact Email:** JB.Simpson@ed.gov

**System Owner**

**Name/Title:** Mindy Chiat / Project Manager

**Program Office:** Federal Student Aid (FSA)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at [privacysafeguards@ed.gov](mailto: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.**

**All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.**

## **1. Introduction**

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

Integrated Student Experience (ISE) (StudentAid.gov) – ISE/StudentAid.gov is a web application designed to be Federal Student Aid’s (FSA) main interface with the public. StudentAid.gov provides students, parents and borrowers with information related to financial aid, navigating through the college decision-making process, applying for federal student aid and repaying student loans.

The ISE/National Student Loan Data System (NSLDS) interface allows, via the “My Federal Student Aid” log in feature provided on StudentAid.gov, federal aid recipients to view their loan and grant information – recipients log in using their FSA ID.

Note: Prior to February 2018, ISE collected and transmitted information for the FSA Ombudsman via the FSA Ombudsman web form – ISE PIA dated 4/22/14. However, in February 2018, the FSA Ombudsman web form was removed from StudentAid.gov.

In future phases, ISE will continue to strategize to seamlessly display FSA applications and content while updating and improving the digital experience for its audience.

1.2 Describe the purpose for which the personally identifiable information (PII)<sup>1</sup> is collected, used, maintained or shared.

PII is not collected or stored in ISE. PII (name, personal financial information) is displayed within ISE for the purpose of providing federal financial aid recipients access to their federal loan and grant portfolio to understand their repayment options, loan servicing contacts, and enable them to make informed decisions about their financial futures.

<sup>1</sup> 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. <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

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? If this is an update, please include the publication date of the original.

Updated PIA

Original Publication Date: 04/04/2014

1.5 Is the system operated by the agency or by a contractor?

Contractor

## 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?

20 U.S.C. 1018(f) (1988).

## 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? Please answer **YES** or **NO**.

Yes

2.2.1  N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).<sup>2</sup> Please provide the SORN name and number, or indicate that a SORN is in progress.

ISE operates under the following System of Records Notice for the National Student Loan Data System (18-11-06).

The SORN is currently being updated but the previously published versions can be found on the Department's SORN webpage: <https://www2.ed.gov/notices/ed-pia.html>

## Records Management

*If you do not know your records schedule, please consult with your records liaison or send an email to [RMHelp@ed.gov](mailto:RMHelp@ed.gov).*

2.3 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Schedule Locator 52. The NARA disposition authority is N1-441-09-21.

<sup>2</sup> 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>

2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

### 3. Characterization and Use of Information

#### Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

PII is not collected or stored within ISE, however ISE displays a user's name and personal financial information during a finite session through the NSLDS web service.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

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

ISE does not collect any data. Information on individuals is displayed.

3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

Individual information is not collected but is shared with ISE by the NSLDS application.

3.5 How is this information validated or confirmed?<sup>3</sup>

Not applicable

<sup>3</sup> Examples include form filling, account verification, etc.

## Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

ISE does not collect or save any PII. PII is only displayed on ISE's web pages for a finite session and not stored in databases, for the use of providing federal financial aid recipients access to their federal loan and grant portfolio to understand their repayment options, loan servicing contacts, and enable them to make informed decisions about their financial futures.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1  N/A If the above answer is **YES**, what controls are in place to minimize the risk and protect the data?

3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1  N/A If the above answer is **YES**, please explain.

### 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.*

3.9 Does the system collect Social Security Numbers? Please answer **YES** or **NO**.

No

3.9.1  N/A If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used. \*Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.\*

3.10  N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

#### 4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The Privacy Policy is appropriately posted for users who are accessing the Studentaid.gov website; this is a general policy serving multiple websites, and no PII is collected within ISE. The policy highlights the voluntary nature of information collected, and explains which data elements are necessary for each level of functionality. Customers are notified that providing the information constitutes consent to all of its uses and they are given no option to affirmatively consent to certain uses. In addition, the policy notifies customers about potential uses of any non-personal information about a visit (i.e., site management data).

4.2  N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

<https://studentaid.ed.gov/sa/privacy>

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Users have the alternative options to access their loan information directly through the NSLDS website or by contacting the Federal Student Aid Information Center. When logging in through PAS, users are presented with a disclaimer explaining the intent of those accessing the system and consents to security monitoring.

## 5. Information Sharing

### Internal

5.1 Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2  N/A What information will be shared and with whom?

The NSLDS data request log information is shared only with the NSLDS team within Federal Student Aid.

5.3  N/A What is the purpose for sharing the specified information with the specified internal organizations?  
Does this purpose align with the stated purpose in Question 1.2 above?

Data request log information is shared to ensure the web service is functioning correctly.

**External**

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

No

5.5  N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

5.6  N/A What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

5.7  N/A How is the information shared and used by the external entity?

5.8  N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

5.9  N/A Does the project place limitation on re-disclosure? Please answer **YES** or **NO**.

## 6. Redress<sup>4</sup>

6.1 What are the procedures that allow individuals to access their own information?

StudentAid.gov has a secure interface within NSLDS that provides the user with their federal loan and grant information. For a user to access their own information, they use their FSA ID user name and password to retrieve their information from NSLDS.

<sup>4</sup> If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

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

Users are instructed to contact the loan servicer. If your attempts to correct your information are unsuccessful, contact the U.S. Department of Education:

Director, National Student Loan Data System, FSA, U.S. Department of Education, UCP, 830 First Street, NE., 4th Floor, Washington, DC, 20202-5454.

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

Procedures are listed directly below loan and grant data on the My Federal Student Aid webpage.

## 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? Please answer **YES** or **NO**.

Yes

7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

ISE system personnel access is granted based on a valid access authorization and intended system usage. The concept of least privilege is employed, allowing only authorized access and privileges for users which are necessary to accomplish assigned tasks in accordance with business functions. In order for federal aid recipients to view their loan and grant information, an FSA ID (a unique user ID and password) is required for logging into StudentAid.gov/MyFederalStudentAid.

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

The Department of Education develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information security and privacy policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures for implementing all required information security and privacy controls. ISE complies with all Education security requirements, as well as the security requirements of the Federal Information Security Management Act of 2002 (FISMA). ISE also complies with the following privacy-related laws and regulations: The Privacy Act of 1974, the E-Government Act of 2002, and various privacy memorandums issued by the OMB.

ISE received a FISMA-compliant Authorization to Operate in July 2018 and conducts monitoring to ensure that the system is operating securely and is employing the appropriate administrative, technical, and physical security safeguards. Examples of controls include, but are not limited to: least privilege/separation of duties; configuration management; risk assessment; physical and environmental protection; identification and authentication; awareness and training; contingency planning/disaster recovery; audit log review; intrusion detection/prevention; firewalls; encryption; security planning; and vulnerability scanning.

7.4 Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

Yes

7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

The ISE application, StudentAid.ed.gov, is part of the Ongoing Security Assessment process at Federal Student Aid which essentially quarterly re-verifies the application's Authority to Operate.

## 8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

The FSA data governance board sets standards for data use, and the system owner ensures that data is used and shared only as allowed by the data governance board, Federal law (including the Privacy Act), and signed agreements.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with this system would result from a breach of security and privacy safeguards as implemented, which could compromise the confidentiality, integrity, and availability of information. The most likely method of a privacy data breach would be through unauthorized access that would enable an adversary to disclose, damage the integrity of, or prevent the availability of information. Privacy risks are mitigated through the Department's continuous security monitoring activities and implementation of all federally required security and privacy controls (more than 150 specific controls).