Privacy Impact Assessment (PIA)

for the

Federal Student Aid Information Center (FSAIC)

May 13, 2020

For PIA Certification Updates Only: This PIA was reviewed on **May 14, 2020** by **Diana O'Hara** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Ashley Jones
Contact Email: Ashley.Jones@ed.gov

System Owner

Name/Title: Diana O'Hara
Principal Office: Federal Student Aid (FSA)

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.

Federal Student Aid's (FSA) Federal Student Aid Information Center (FSAIC) system is a multichannel customer contact center that performs all functions associated with receiving and responding to inquiries, including telephones, telecommunication devices for the deaf (TDD/TTY), email, fax, postal mail, web chat, social media, text messaging, and other media as appropriate. The FSAIC provides information and assistance to potential and current students, parents, as well as counselors, schools, and other public inquirers. FSAIC assists customers nationally and internationally with questions on a wide range of topics throughout the entire financial aid process, including preparing for college, the types of student aid, aid eligibility, applying for aid, and managing student loans.

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

FSAIC system collects and maintains PII to:

a. Assist FSAIC Customer Service Representatives (CSRs) in properly documenting the interaction with FSAIC customers and to provide the necessary contact information so that CSRs can perform follow up activities with the customer.

b. Implement CSRs quality monitoring process so that the quality team can monitor and provide feedback and training to the CSRs on their interactions with FSAIC customers.

c. Verify the identity of the customer as well as to access the FSAIC customers' information in other FSA applications such as Person Authentication Service (PAS), Central Processing System (CPS), and National Student Loan Database System (NSLDS).

All PII collected through FSAIC is ultimately stored in CPS. For more information please refer to the CPS PIA. The CPS PIA can be found here:

[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

https://www2.ed.gov/notices/pia/cps.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?

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 Higher Education Act of 1965 (Public Law 89-329), as amended, sections 428,484, and 485B; 31 United States Code (U.S.C). 7701; and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

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

While the information in FSAIC is not retrieved by a personal identifier, once it is moved to CPS, it is retrieved by an identifier. Therefore, this information is covered under the Federal Student Aid Application File System, 18-11-01, which was last published in the Federal Register on November 29, 2019.

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

Click here to enter text.

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.

The Department shall submit a retention and disposition schedule that covers the records contained in this system to NARA for review. The records will not be destroyed until such a time as NARA approves said schedule.

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

[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

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.

Name (first, last and middle initial), Social Security number (SSN), date of birth (DOB), street address, telephone number, and/or email address may be requested/collected to authenticate an individual's identity when they contact FSAIC.

Depending on the purpose for contacting FSAIC, additional PII data elements may be requested/collected such as driver license number and state of issuance, citizenship status, marital status (including month and year of marriage), state of legal residence, date of legal residency, if applicable, sex/gender, and education level

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

Yes

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

PII is collected directly from students and parents.

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 collected is either through on-line chats on studentaid.gov (Customer Relationship Management (CRM)), phone (audio), and/or in paper-form (fax and/or postal mail Control Correspondence).

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?

When PII is provided to FSAIC CSRs, the CSRs validate the information provided with records in FSA's Central Processing System. All additional information that may be collected will be validated by CPS.

For more information on how CPS validates the information maintained, please refer to the CPS PIA.

[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.

Use

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

FSAIC system collects, maintains, and uses PII to:

a. Assist CSRs in properly documenting the interaction with FSAIC customers and to provide the necessary contact information so that CSRs can perform follow up activities with the customer; and

b. Verify the identity of the FSAIC customer as well as to access FSAIC customers' information in other FSA applications such as PAS, CPS, and NSLDS.

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.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

SSN being a unique identifier for Title IV programs, its collection and use is required to verify the identity of the FSAIC customer as well as to access the FSAIC

customers' information in other FSA applications such as PAS, CPS, and NSLDS and assist FSAIC customers with their questions on a wide range of topics throughout the entire financial aid process.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

FSAIC considered alternatives to SSNs (such as First and Last Name). However, an SSN is a unique identifier for Title IV programs.

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.

There is a link on the "Contact Us" page that takes the user directly to both the Privacy Act notice and the privacy policy. Additionally, a privacy notice is read aloud over the phone at the beginning of all conversations.The Privacy Act notice, and the privacy policy are located at: https://studentaid.gov/notices/privacy.

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

https://studentaid.gov/notices/privacy

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?

If you decide to call one of the contact centers listed on our "Contact Us" page you will be asked to provide information in order to authenticate your identity which may include your name, date of birth, SSN, or other identifying information to distinguish you from another individual.

All interactions over the phone are completely voluntary. Failure to provide authenticating information will prevent the user from receiving information regarding their loan or grant.

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.

[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 applicant has the ability to access their records through interactions with the CSR. Alternatively, individuals may access their records online with their FSAID.

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

The applicant has the ability to amend their records through interactions with the CSR. The applicant also has the ability using their FSAID to pull up their application and make corrections or they can work with the Financial Aid Administrator who can assist with correction to the application.

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

Information regarding procedures for correcting records is provided on the FAFSA application, on the StudentAid.gov website, and through the publication of the SORN referenced in 2.2.1 and this PIA. Additionally, if an individual contacts FSAIC, a CSR can inform them of these procedures as well.

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?

In accordance with the Federal Information Security Modernization Act (FISMA), every FSA system must receive a signed Authority to Operate (ATO) from a designated ED official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. Privacy risks are mitigated by encrypting and/or masking the customers' PII and/or by controlling access to the customer information on a need to

know basis as well as by requiring two-factor authentication. Additionally, devices on which the customers PII are stored are maintained in secured server rooms with limited physical access to authorized personnel only. Intrusion Prevention Systems (IPS) and Firewall devices are also in place to protect access to this information. All FSAIC personnel are also required to obtain a public trust security clearance, sign the FSAIC Rules of Behavior document, and to complete security awareness training on an annual basis.

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.

All CSR phone conversations, chats, and action are recorded and reviewed for quality control on a regular basis with management to ensure PII is being handled appropriately. All PII collected through interactions with FSAIC and stored in CPS. For additional information on monitoring, testing, and evaluation, please refer to the CPS PIA.

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 FSAIC system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology, which addresses security and privacy risks throughout the FSA system's lifecycle. Additionally, the system owner ensures that quality control processes are sufficiently implemented to ensure the stated practices in this PIA are followed.

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?

The privacy risks associated with the FSAIC is the inadvertent or malicious compromise of the confidentiality and integrity of the individual's personal information. This is mitigated by ensuring all CSRs authenticate and verify an individual's identity in multiple ways. They are encouraged to utilize all means necessary including advising an individual to visit their FSA Administrator at their university in person. All major changes to a PII data element are verified in multiple ways and can be reported to management for review. Additionally, adequate security controls are in place to provide reasonable assurance that the individual's confidentiality and integrity of the individual's personal information is not compromised when maintained by the Department.