Privacy Impact Assessment (PIA) for the Federal Student Aid Information Center (FSAIC)

Oct 6, 2017

This PIA was approved on Oct 6, 2017 and reviewed on Oct 6, 2017 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Mr. Shital M. Shah, FSAIC Information System Security Officer
Contact Email: shital.shah@ed.gov

System Owner

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

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.

All text responses are limited to 2,000 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

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

Federal Student Aid (FSA) Federal Student Aid Information Center (FSAIC) system is a government call/contact center that performs all customer service functions associated with receiving and responding to potential and current Free Application for Federal Student Aid (FAFSA) applicants such as students, parents, as well as counselors, schools, and other public inquirers (herein collectively referred to as FSAIC customers) 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 through the use of various communications media, including telephones, telecommunication devices for the deaf (TDD/TTY), email, fax, postal mail, web chat, social media, and other media as appropriate.

1.2 □ N/A Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained or shared.

FSAIC system collects, maintains, and uses FSAIC Customers’ PII to:
• 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.
• 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.
• Verify the identity of the FSAIC customer as well as to access FSAIC customers’ information (including the loan information as per the Higher Education Act of 1965 (Public Law 89–329), as amended) in other FSA applications such as PAS, CPS, and NSLDS.

1.3 □ N/A Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 □ N/A 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: 10/16/2016

1.5 □ N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

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.

If you are unsure of your legal authority, please contact your program attorney.

2.1 □ N/A  What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

- 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).

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.

SORN

2.2 □ N/A 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)). Please provide the SORN name and number, or indicate that a SORN is in progress.

The FSAIC is covered by Federal Student Aid Application File System of Records Notice, (SORN) # 18-11-01 (76 FR 46774-81).

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 □ N/A 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.

FSA is working with the Department of Education Records Officer and The National Archives and Records Administration (NARA) to obtain the appropriate retention value.

2.4 □ N/A 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.

[ ] No

3. Characterization and Use of Information

Collection

3.1 □ N/A 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.
The FSAIC customer PII collected, used, or maintained could be any of the following elements or a combination thereof:

- Social Security number (SSN),
- Name (first, last and middle initial),
- Date of Birth (DOB),
- Street Address,
- Telephone number,
- Email Address,
- 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,
- Education level.

3.2 □ N/A 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 □ N/A What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

The sources of PII are Students (and his/her spouse, if applicable) and parental information for dependent students as well as counselors, schools, and other public inquirers.
3.4 N/A How is the information collected from stated sources (paper form, web page, database, etc.)?
The PII collected is either through Customer Relationship Management (CRM) application (Control
Correspondence) or phone (audio) and video (desktop) recordings.

3.5 N/A How is this information validated or confirmed?
FSAIC validates or confirms the collected PII via verification of the data presented with the end user.

Use
3.6 N/A Describe how and why the system uses the information to achieve the purpose stated in
Question 1.2 above.
FSAIC system uses FSAIC Customers' PII to;
• 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.
• 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.
• Verify the identity of the FSAIC customer as well as to access FSAIC customers’ information (including
the loan information as per the Higher Education Act of 1965 (Public Law 89-329), as amended) in other
FSA applications such as PARS, CPS, and NSLDS.

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

Yes

3.7.1 N/A If the above answer is YES, what controls are in place to minimize the risk and
protect the data?
All FSAIC environments such as testing, production, etc. -- are protected by the security and privacy
controls required by FISMA and the Privacy Act.

3.8 N/A 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.

3 Examples include form filling, account verification, etc.
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 ☐ N/A Does the system collect Social Security Numbers? Please answer YES or NO.

Yes
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.*

Social Security Number (SSN) is 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.

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

FSAIC had considered to use alternative (such as First and Last Name) to collection of SSN#. However, SSN# is 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.

4. Notice

4.1 □ N/A 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 CRM on-line application contains a detailed Privacy Act notice. The customer data referred to during FSAIC customer service calls originates from the Free Application for Federal Student Aid (FAFSA); the FAFSA website (www.studentaid.ed.gov) contains a detailed Privacy Act notice. Additionally, the prompt within the FSAIC telephony/Integrated Voice Response (IVR) system discloses to the customers that their calls may be recorded for quality purposes.

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

The following sub-bullets are the two FSAIC web addresses and the privacy notice for those web addresses is located at https://studentaid.ed.gov/sa/privacy.
- https://studentaidhelp.ed.gov
- https://studentaidhelp-es.ed.gov/app/home

4.3 □ N/A What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?
FSAIC CSRs follow canned scripts/processes to assist end users with the student aid process and they confirm the end user's identify by asking them to provide elements of PII such as their first and last name, SSN, and DOB. The end user can either consent to provide this information so that the FSAIC CSR can assist them or they can decline in which case the FSAIC CSR will not be able to assist them. The end user also has the opportunity to consent to provide the requested information to verify their identity when utilizing the FSAIC IVR for self-help purposes.

During interactions with FSAIC CSRs, the end user has the ability to decline to provide the FSAIC CSR with the information requested. In these cases the FSAIC CSR will not be able to assist the end user. The end user also has the ability to decline to provide the information requested by the FSAIC IVR in which case the FSAIC IVR will provide a canned response that information cannot be provided and will close the call. During interactions with FSAIC CSRs, the end user also has the ability to opt out of the project. In these cases the FSAIC CSR will not be able to assist the end user. The end user also has the ability to opt out/not provide the information requested by the FSAIC IVR in which case the FSAIC IVR will provide a canned response that information cannot be provided and will close the call.

5. Information Sharing

Internal

5.1 □ N/A 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?

Control correspondence information captured via the CRM application is only accessible by/shared with authorized FSA and contractor personnel. The information captured during the desktop and audio recording process is shared with FSA personnel.

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?

Control correspondence information is shared with authorized FSA personnel so they can review and authorize the responses. Information captured via the desktop and audio recording processes, are shared with authorized FSA personnel to assist in the quality monitoring and training of FSAIC CSRs.

External

5.4 □ N/A 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 internal 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.

Yes
6. Redress

6.1 □ N/A  What are the procedures that allow individuals to access their own information?
Procedures for allowing individuals to access their own information are explained in the System of Records notice listed in question 2.2.

6.2 □ N/A  What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?
Procedures for allowing individuals to access their own information are explained in the System of Records notice listed in question 2.2.

6.3 □ N/A  How does the project notify individuals about the procedures for correcting their information?
The System of Records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1 □ N/A  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 □ N/A  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?

Access to FSA information is governed by the concepts of least privilege and separation of duties. All system access is granted by predefined roles and privileges, and all FSA system users must undergo a Federal background security clearance process.

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

FISMA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, 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, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

4 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.
7.4 □ N/A  Is an Authority to Operate (ATO) required? Please answer YES or NO.

[ ] Yes

7.5 □ N/A  Is the system able to provide account of any disclosures made? Please answer YES or NO.

[ ] Yes

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

DXC/ES Security team test and validate
a. The Oracle cloud services (ORSC) Customer Relation Management (CRM) application security controls when Oracle rolls out software releases to their Oracle Service Cloud SaaS offering.
b. The Call Recording infrastructure components before the changes are made to the FSAIC production environment.
Access to FSAIC assets (components as well as information) is monitored on a weekly basis via the review of ArcSight and End Point Threat Management (EPTM) reports as well as quarterly review of auditing and attestation of FSAIC user accounts.

8. Auditing and Accountability

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

The 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 system’s lifecycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of Records notices, memoranda of understanding, etc.

8.2 □ N/A What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks are mitigated by masking the customers’ PII entered within the FSAIC CRM application. Data at rest stored within the FSAIC CRM is encrypted using FIPS-validated methods. Access to customers’ PII stored within the FSAIC CRM is further controlled on a need to know basis as well as by requiring two-factor authentication. The call recordings are also encrypted while stored at rest and are maintained on servers located within secured server rooms with limited physical access to authorized personnel only. These servers are not internet accessible and are further protected by Intrusion Prevention Systems (IPS) and firewalls. All FSAIC personnel are 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.