Privacy Impact Assessment (PIA)
for the

MyStudentAid
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.

    myStudentAid (mySA) is a mobile-centric application used by students and their parents to submit their post-secondary applications for Title IV student financial aid (grants and loans) based on the Free Application for Federal Student Aid (FAFSA) process. This is an alternative to completing the FAFSA application on paper or on the FAFSA.gov website. This application directly feeds the Central Processing System (CPS) with the applicant's information. The applicant information is only stored in CPS. The CPS PIA can be found here: https://www2.ed.gov/notices/pia/cps.pdf.

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

    The myStudentAid mobile application provides an alternative method for applicants to apply for Federal student aid. PII collected on the FAFSA application via the myStudentAid mobile application is stored in CPS. The CPS uses the applicant's PII to help determine an applicant's eligibility for Federal Financial Aid.

    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] 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

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, As Amended, The Higher Education Act of 1965 (HEA), as amended, Section 441 and 461 Title IV, Section 401Section 1001 et seq.

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 the myStudentAid application 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](#)), was 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.

---

[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

☑ 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
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.

The myStudentAid mobile application collects and transmits FAFSA applicants' personal information such as:

Full name (first, last, and middle initial); applicant's and parent's Social Security number (SSN); date of birth; address; telephone number; personal email address; financial information, including information obtained through use of the Internal Revenue Service's Data Retrieval Tool (DRT), additional user profile data such as institution of higher education to share application with.

For more detailed information on the specific data elements collected, please refer to the Central Processing System PIA.

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 applicant and parents whose information is being provided.

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 information is collected through the myStudentAid mobile application from the applicant and/or parent and it is self-reported.

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 an applicant fills in their information there are content requirements for various fields such as for SSNs. While completing the application, data is further validated if an applicant chooses to use the Internal Revenue Service's (IRS) Data Retrieval Tool (DRT).

Any information that is collected through the myStudentAid application is transmitted to CPS for further validation with other FSA information systems and Federal agencies.

Use

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

The personal information collected via the myStudentAid mobile application is sent to the CPS. CPS uses the individual's information to determine an applicant's eligibility for Federal Financial Aid and notifies students and educational institutions of the results of the eligibility calculation.

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

---

[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.

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

Social Security Numbers are a unique identifier for Title IV programs, its collection and use are required for the purpose of determining an applicant's eligibility for Federal Financial Aid. Additionally, use of the SSN is required as the unique identifier by other external partners involved in determining eligibility for Federal student aid throughout the student aid lifecycle..

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

☐ N/A

myStudentAid considered alternatives to SSNs (such as First and Last Name). However, an SSN is a unique identifier for Title IV programs, and its collection and use are required for the purpose of determining an applicant's eligibility for Federal Financial Aid. Moreover, CPS performs the verification of SSNs with the Social Security Administration (SSA) to uniquely identify students, and students are required to validate that the SSN and other information entered is correct.

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, prominently displayed, within the MyStudentAid Application that takes users directly to both the Privacy Act Notice and the Privacy Policy.

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

The Privacy Act notice and the privacy policy for the FAFSA application are located at: 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?

Individuals provide their PII voluntarily in order to receive aid. The myStudentAid application collects no personal information about the individual unless the individual chooses to provide the information. If individuals decline to provide their personal information, or if there is missing applicant information, the FAFSA form may not be processed or the applicant aid may be delayed or denied. If the applicant wants federal student aid only, the applicant does not have to answer certain questions. However, if the applicant wants to apply for state financial aid, the applicant must answer all the relevant questions.

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

While the information is collected by myStudentAid application, once it is moved to CPS, it may be shared with external entities. For information about how this information is shared externally, see SORN referenced in 2.2.1 and the CPS PIA.

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

---

[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.

5.9. 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?

   While in the process of completing the FAFSA, individuals may access their information through the use of the myStudentAid mobile application or by logging onto studentaid.gov with their FSA ID.

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

   The applicant has the ability, using their FSAID, to pull up their application through the mobile app 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?

   There are online help text and instructions on the web site (https://fafsa.ed.gov/help.htm) to assist individuals on the process of application submission, next steps, correcting 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?

   myStudentAid is built on a secure infrastructure that is FedRAMP-compliant and agency authorized and is managed using a system development life cycle methodology that includes information security considerations, following an agile, iterative development model using the SCRUM framework. myStudentAid meets the current NIST SP 800-53 security controls for moderate systems and was assessed through the formal Authority to Operate (ATO) process. FSA conducts user account reviews on a quarterly basis, reviewing user access granted within the information system. User access reviews help to identify, including but not limited to:
   - A terminated employee gaining remote access to the network or email system;
   - Segregation of duties issues;
   - Misuse of dormant administrative accounts that are still active; and/or
   - System compromise using vendor passwords.

   The myStudentAid mobile application requires an up to date operating system on the device that it is downloaded to and has similar log-in requirements to accessing the FAFSA application through a web browser including two factor authentication. All data is encrypted.

   All collected PII is stored in CPS, the protection mechanisms for the stored PII are documented in CPS PIA.

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.

As part of the ATO process, a FSA approved third party assessor performs a rigorous assessment of myStudentAid security controls. Plan of actions and milestones (POA&M) are developed and implemented to ensure that all identified deficiencies are remediated. myStudentAid is enrolled in FSA Continuous Monitoring program where the security controls are tested and evaluated on a quarterly basis to ensure that the controls are working as intended. Vulnerability scans are also conducted and patches are deployed regularly.

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 myStudentAid 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. The system owner for myStudentAid is also responsible for CPS where the PII collected through the mobile application is stored. This allows for consistency of privacy and security safeguards.

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 myStudentAid system is the inadvertent or malicious compromise of the confidentiality and integrity of the individual's personal information. However, 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. myStudentAid is a mobile-centric application used by students & parents to submit their post-secondary applications for Title IV student financial aid based on the Free Application for FAFSA. myStudentAid does not store (contain) any PII. It collects the students and parents FAFSA (including PII) information and forwards the collected FAFSA information to FSA Central Processing System via FSA Enterprise Service Bus (ESB) for further processing. This prevents compromise in the event a mobile device is physically or electronically compromised.