Privacy Impact Assessment (PIA)

for the

Central Processing System (CPS)

April 21, 2020

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

Contact Point

Contact Person/Title: Nina Colón, Information System Security Owner
Contact Email: Nina.colon@ed.gov

System Owner

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

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 Central Processing System (CPS) is the automated system that processes all Free Application for Federal Student Aid (FAFSA) submissions for Federal Student Aid (FSA) for the U.S. Department of Education (Department). CPS calculates financial aid eligibility and notifies applicants and educational institutions of the results of the eligibility calculation. CPS also performs image and data capture of paper applications, develops and manages the mainframe eligibility determination system, provides Web-based applications and services, develops personal computer (PC) based financial aid software, prints and mails eligibility documents and supports the Participation Management (PM) system for FSA title IV programs.

CPS is comprised of several technological and operational components. They include:

- Business Intelligence (BI) Tool
- Eligibility Determination System (EDS)
- FAA Access to CPS Online
- FAFSA on the Web
- Image and Data Capture (IDC)
- CPS Printing Component
- FSA ID
- Participation Management (PM) System
- EDExpress for Windows
- Direct Loan Tools
- IRS Datashare System

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

CPS is the initial stage of the Student Aid Lifecycle responsible for determining an applicant's eligibility for Federal financial aid. PII is collected on the FAFSA application

[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

and maintained in CPS to verify the identity of an applicant and the parents of a dependent applicant in order to determine, process, and track eligibility requirements and determinations.

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.

Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. 1070 et seq.). The collection of Social Security numbers (SSNs) of users of this system is also authorized by 31 U.S.C. 7701 and Executive Order 9397, 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?

Yes

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

Federal Student Aid Application File (18-11-01) most recently published in the Federal Register on October 29, 2019 at 84 FR 57856-57863.

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

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

The elements of PII data collected and maintained by the system include but are not limited to:

A. Applicant (and spouse, if applicable, and parental information for dependent applicant) personal information.

   Personal information is collected and used to uniquely identify the applicant and determine if the applicant meets the eligibility requirements for Federal Student Aid. Personal information collected includes but is not limited to: Social Security Number (SSN), name (first, last and middle initial), address, date of birth (DOB), telephone number, driver license number and state of issuance, email address, citizenship status or alien registration number (if applicable), marital status (including month and year of marriage), state of legal residence, date of legal residency, if applicable, sex,.

   Pursuant to Computer Matching Agreements (CMA) between Federal Student Aid and other Federal agencies, the Department may also maintain the following PII elements. For more information please refer to the Department's CMA webpage: https://www2.ed.gov/about/offices/list/om/pirms/cma.html

   From the Department of Homeland Security's United States Citizenship and Immigrations Services (DHS-USCIS): Verification case number, date of entry into the United States, country of birth, DHS-USCIS status code, and eligibility message code.

   From the Department of Defense (DoD): Dependent's name, date of birth, SSN whose parent or legal guardian died as a result of U.S. military service in Iraq or Afghanistan after September 11, 2001 and the date of death of the parent of guardian.

   From the Department of Justice (DOJ): name and SSN of individuals who do not qualify for Federal student financial assistance under the Controlled Substances Act, as amended, the title IV programs included under court sanction, the end date of the debarment period, and the codes for the denied Federal benefits.

   From the Social Security Administration (SSA): a match indicator to confirm valid SSN or citizenship.

   From the Selective Service System (SSS): a match indicator to confirm registration with the Selective Service

From the Department of Veteran's Affairs (VA): a match indicator referencing Veteran status.

B. Dependency Status

Dependency status questions on the FAFSA determine whether parents' income and asset information will need to be included on the application. These questions include but are not limited to: applicant's age, education level, marital status, dependents and the amount of parental support, active duty status, and veterans status.

C. Applicant's Income, Tax Credit, and Asset Information

The following information is collected for the applicant (and spouse): Federal income tax return information, adjusted gross income (AGI), income tax paid, number of exemptions, income earned from working (wages, salaries tips), and untaxed income. Asset information includes cash, savings, and checking account balances, investments, and the net value of businesses and/or investment farms.

D. Dependent Applicant's Parental or Legal Guardian Information

The following information is collected for the applicant's parent(s): Parent(s) highest level of schooling completed, marital status, marital status date (month and date), SSN(s), last name(s) and first initial(s), date of birth, email address, number in Household supported by the parent(s), state of legal residence, date of legal residence, Federal income tax return information, adjusted gross income (AGI), income tax paid, number of exemptions, income earned from working (wages, salaries tips), and untaxed income. Asset information includes cash, savings, and checking account balances, investments, and the net value of businesses and/or investment firms.

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.)?

The main source of the information is the applicant and/or parent, and it is self-reported. Data are collected directly from the student/parent when they submit the Free Application for Federal Student Aid (FAFSA).

If the applicant is a current or previous borrower, their previous application information can be pulled from the National Student Loan Database System (NSLDS) to assist in application completion.

Additional sources include the Federal agencies through which FSA conducts a computer matching agreement with including DHS, DoD, DOJ, SSA, SSS, and VA.

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 is collected via the FAFSA on the Web application submission form on FAFSA.gov, the mobile application, a paper form or via FAA Access by the school Financial Aid Administrator working with the applicant and parent to complete the FAFSA application or make corrections on the students' application.

Information obtained from other Federal agencies is obtained through a computer match. For more information please reference the specific matching agreements at: https://www2.ed.gov/about/offices/list/om/pirms/cma.html

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 the application data is submitted to the Central Processing System the data is ran through system edits for data accuracy. For example, all data submitted to CPS is validated against data in NSLDS if an applicant is a previous borrower.

When an applicant completes the FAFSA form, there are also content requirements for various fields such as for SSNs. Additionally, during the application process data is further validated through an applicant's use of the Internal Revenue Service's (IRS) Data Retrieval Tool (DRT).

[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.

Additional checks on data integrity occur when PII is sent to match with other Federal Agencies pursuant to the matching programs listed above. Matches occur on a regular basis ranging from daily to quarterly depending on the current Computer Matching Agreement.

Use

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

CPS is the automated system that processes all FAFSA submissions for Federal Student Aid for the Department and uses PII to validate the identity of applicants. CPS uses an applicant's PII to calculate financial aid eligibility and notify the individual and respective educational institutions of the results of the eligibility calculation. Throughout the eligibility determination process, the PII is checked through various systems and processes to assist applicants in completing their application, ensure they provide accurate information, and are offered the benefits they are entitled to.

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

SSNs are collected and used for the purpose of authenticating a user's identity. SSNs are also used as an authoritative source of identity when determining eligibility pursuant to various computer matching agreements with other Federal agencies.

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

☐ N/A

There are no alternatives to consider for the collection of the SSN--SSNs are matched with SSA to uniquely identify students. A valid SSN is required by SSA as the unique identifier for students, parents, and financial aid professionals. Additionally, use of the SSN is required as the unique identifier by other external partners involved in determining eligibility for Federal student aid, such as the Internal Revenue Service (to use the IRS Data Retrieval functionality within the FAFSA on the Web application), and other Federal agencies with whom the Department conducts a computer match.

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.

A Privacy Act Statement is provided before the student or parent completes the FAFSA. This notice is provided both on the FAFSA website and the paper version of the FAFSA.

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?

Applying for FAFSA is purely voluntary but if requested information is not provided by the applicant or information is missing, the application cannot be processed and will delay the process of determining the applicant's eligibility for any aid.

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.

Yes

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

[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.

CPS shares basic identifiers such as name, SSN, and date of birth with six other Federal agencies pursuant to computer matching agreements: DHS, DoD, DOJ, SSS, SSA, and VA.

Additionally, PII including but is not limited to: SSN, DOB, legal addresses, first and last names, and email addresses may be shared with guaranty agencies, financial institutions participating in Federal Family Education Loan (FFEL) programs, institutions of higher education, third party servicers, Federal, State, and local agencies, fiscal agents designated by Treasury, and consumer reporting agencies.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

PII is shared with 6 different Federal agencies pursuant to a Computer Matching Agreement including: SSA to verify the SSNs and confirm the U.S. citizenship status, or date of death of applicants and dependent applicant's parents; VA to verify the veteran status of applicants; SSS to confirm the registration status of male applicants; DHS-USCIS to confirm the immigration status of applicants; DOJ to enforce any requirement imposed at the discretion of a court for a drug-related offense; DoD to identify dependents of U.S. military personnel who died in service in Iraq and Afghanistan after September 11, 2001, to determine if they are eligible for increased amounts of title IV, HEA program assistance. For more information on the Computer Matching Agreements conducted with records in CPS please see: https://www2.ed.gov/about/offices/list/om/pirms/cma.html

PII may be disclosed pursuant to one of the following programmatic disclosures published as a routine use in the SORN as referenced in 2.2.1.

- To verify the identity of the applicant and the parent(s) of a dependent applicant; determine the accuracy of the information contained in the record; support compliance with title IV, HEA statutory and regulatory requirements; assist with the determination, correction, processing, tracking, and reporting of program eligibility and benefits; enable an applicant, to obtain information from other Federal agencies' records; determine an applicant's eligibility for the award of State postsecondary education assistance and for the award of aid by eligible IHEs or other entities or expedite the student application process.
- To provide an applicant's financial aid history, including information about loan defaults and grant program overpayments.

- To facilitate receiving and correcting application data, processing Federal Pell Grants and Direct Loans, and reporting Federal Perkins Loan Program expenditures to the Department's processing and reporting systems.
- To enforce the terms of a loan or grant; assist in the collection of loan or grant overpayments; or assist loan holders with the collection and servicing of loans, to support pre-claims/supplemental pre-claims assistance.
- To facilitate assessments of program compliance and assist in assessing the administration of program funds by guaranty agencies, financial institutions, IHEs, and third-party servicers.
- To assist borrowers in repayment, or the Department in locating borrowers or loan holders.
- To initiate legal action against an individual involved in an illegal or unauthorized program expenditure or activity; initiate or support a limitation, suspension, or termination action, an emergency action, or a debarment or suspension action; or investigate complaints, update files, and correct errors.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

The information is shared electronically outside the Department over secure, encrypted Networks.

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

Yes

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

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

Individual users may access their own application data using the FSAID that is created when the individual starts the FAFSA application. The user can login with credentials and FSAID and access their Federal Student Aid data on file. Users currently enrolled in an educational institution can also contact their Financial Aid Administrators for access to their records maintained in CPS.

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

The applicant may use their FSAID to pull up their application in FAFSA Corrections on the Web or they can work with the Financial Aid Administrator that can assist with correction to the application. If applicant uses the IRS Data Retrieval Tool to automatically populate the FAFSA application with their tax data, the data fields will be masked. The masking of the fields is for security purposes and is not a field that can be altered. The tax fields that have been populated by the IRS DRT will not be able to be changed but individuals are able to manually provide their information.

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

Once the applicant has submitted the application and data has been processed an email will be sent to the applicant with instructions on how to access the application data and instructions on how data can be corrected if necessary. The application also has online help text and instructions on the web site to assist individuals on the process of application submission and next steps.

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?

CPS meets the current NIST SP 800-53 security controls for moderate systems and was assessed through the formal Authority to Operate (ATO) process. FISMA controls implemented comprise a combination of management, operational, and technical controls. CPS is only accessible to users that meet the minimum security clearance requirements and have been granted access to the internal Department network. Network access is annually granted once users complete the required Cybersecurity and Privacy Awareness Training. Access is further controlled by the Information System Security Officer (ISSO) and all users are required to utilize two factor authentications follow a complex password policy, and read and accept a Rules of Behavior. All data is encrypted in transit and at rest and physical access to the Department's and its contractor's locations are controlled an monitored by security personnel.

For external users who are not Department employees access is strictly controlled and secured through the use of multifactor authentication. All users are authenticated through FSA's Access and Identity Management System.

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.

CPS is required to obtain and maintain an Authorization to Operate (ATO). This process includes a tri-annual independent assessment of all required security and privacy controls and produces Plans of Actions and Milestones (POAMs) to ensure any deficiencies are remediated. The CPS System also participates in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security controls are in place and working properly. CPS has a regular patching cycle to ensure the system is secured with the most up to date capabilities. Following each patch release an additional scan is conducted to ensure continuing operations. Additional activities include conducting regular self-assessments, contingency plan testing and participating in tabletop exercises.

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 system owner along with the ISSO ensure that the data collected is maintained and used in accordance with the stated practices in this PIA. The first method is by completing the Department of Education Risk Management Framework process in order to receive an Authority to Operate (ATO). During the ATO process the security controls were assessed by an independent assessor to ensure the CPS and its data are appropriately secured and protected. The second method was making sure that the National Institute of Standards and Technology (NIST) 800-53 controls are implemented by CPS. The NIST controls comprised of administrative, technical and physical controls to ensure that the information is used in accordance with approved practices. The third method is by ensuring that the system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Life-cycle Management Methodology, which address security and privacy risks through the system's lifecycle.

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 main privacy risk is unauthorized access or use of the data, which could lead to identity theft, financial fraud, and loss of public trust. These risks are mitigated through strict access controls and the deployment of various tools that prevent the loss of data.

An additional risk is to privacy is maintaining inaccurate information which could result in inaccurate eligibility determinations. This risk is mitigated by validating the PII at various levels of the eligibility determination process. This is accomplished by entering into computer matching agreements with other Federal agencies and validating returning applicant information against the PII currently maintained in NSLDS.