Privacy Impact Assessment (PIA)

for the

Central Processing System (CPS)

April 10, 2017

Contact Point

Nina Colon

202-377-3384

System Owner

Diana O'Hara

Author

Nina Colon

Office of Federal Student Aid
Customer Experience Group

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 information in identifiable form 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.*

Introduction

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

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 (the Department), calculates financial aid eligibility and notifies students 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 a number of 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.

[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.
https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

PII data is collected on the FAFSA application and used to help determine an applicant's eligibility for Federal Financial Aid. The applicant's data is matched against other Federal Agency systems to determine that the applicant meets the federal regulations' eligibility requirements to receive Federal student aid. The federal agency system matches include: Social Security Administration, Veterans Administration, Selective Service, Department of Justice, Department of Defense, and Department of Homeland Security. The data is housed in the Central Processing System DB2 which is hosted at the NTT Data Center in Plano, Texas.

1.3. Is this a new system, or one that is currently in operation?

The CPS is currently operational.

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

This PIA is an update of a previous version.

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

CPS is operated by contractors. GDOS is application Developer contractor and NTT is the Data Center contractor that hosts the CPS System Mainframe and Midrange Environments.

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?

The Higher Education Act of 1965, As Amended, Section 1001 et seq.

SORN

2.2. Is the information in this system retrieved by name or personal identifier? If so this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s))[2]? If no, explain why not. If yes, provide the SORN name and number, or indicate that a SORN is in progress.

[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

A system of records has been created for this collection of information. Users are provided notice of their rights under the Privacy Act of 1974 via links to the agency Privacy Act regulations (5 C.F.R. Part 5b) and to the Privacy Act system of records notice for the website. The original notice, entitled "Federal Student Aid Application File" (18-11-01), was published in the Federal Register on June 1999 (64 FR 30159). This notice has been amended several times since its original publication; the most recent amended version was published in the Federal Register on August 3, 2011 (76 FR 46774).

Records Management

If you do not know your records schedule, please consult with your records liaison or RMHelp@ed.gov.

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

CPS has two records retention and disposition schedule numbers from NARA: NARA Job No. NC-12-75-1 and NARA Job No. NC 12-80-2 and GRS 20.

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

A. Student (and spouse, if applicable, and parental information for dependent students) personal information

Personal information is collected and used to uniquely identify the student and determine if the student 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, data of birth (DOB), telephone number, driver license number and state of issuance, email address, citizenship status, marital status (including month and year of marriage), state of legal residence, date of legal residency, if applicable, sex, Selective

Service registration status, education level and whether applicants have been convicted of possessing or selling illegal drugs while receiving Federal student aid.

B. Dependency Status

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

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

The following information is collected for the student (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 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 farms.

The sources of information collected come from students, parents (if applicable), employees and institutions. The information is collected via the FAFSA on the Web application, submission of a paper form website, paper form that can be printed from the website, via FAA Access by the school, or via the Federal Student Aid Information Center (FSAIC) help desk (FAFSA on the Phone submissions).

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

The FAFSA form collects the minimum information necessary to achieve the purpose stated in the introduction.

3.3. What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.), how is the information collected from stated sources (paper form, webpage, database, etc.), and how is this information validated or confirmed?[3]

The source of the information collected is from the student and/or parent and it is self-report.

Use

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

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 (the Department), calculates financial aid eligibility and notifies students and educational institutions of the results of the eligibility calculation.

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 the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.5. Does the system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures. *Please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.*

SSNs are collected and used for the purpose of authenticating a user's identity. The HEA Act of 1965 and Privacy Act of 1974 provide the disclosure information.

3.6. Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

There are no alternatives to consider for the collection of the SSN--SSNs are matched 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. 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), Veterans Administration, and the Selective Service Administration.

[3] Examples include form filling, account verification, etc.

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.

In addition to agency matches, we also have web edits for online applications to ensure accuracy before submission, compute edits when processing paper and electronic records, and a verification selection process to identify records that are most likely error-prone to be selected for verification.

4.2. Provide the text of the notice, or the link to the webpage where notice is posted.
https://fafsa.ed.gov/privacy.htm

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

We collect no personal information about the applicant unless the applicant chooses to provide that information to us. If we do not collect the information form the applicant or if there is missing applicant information we can't process the application, which will delay the process of determining the applicants eligibility for any aid.

5. Information Sharing

Internal

5.1. Will information be shared internally with other ED organizations, if so, which ones?

In accordance with requirements set forth by the Department the CPS shares information with the Department to allow it to administer the Federal student aid programs. The Department may disclose information contained in a record in an individual's account in accordance with the Privacy Act of 1974. CPS shares information with:

- Federal Student Aid and its agents or contractors
- National Student Loan Data System (NSLDS)
- Postsecondary Educational Participants System (PEPS)
- Common Origination and Disbursement System (COD)
- Student Aid Internet Gateway (SAIG)

5.2. What information will be shared and with whom?

The information shared is sensitive student level data as it pertains to students applying and receiving Title IV aid from FSA. The Department may disclose information in this system

without the consent of the individual, in accordance with the provisions of the Privacy Act of 1974.

5.3. 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?

The purpose of the information sharing is to perform internal system monitoring, student tracking, payment allocation and historical records and review. This purpose aligns with the purpose in Question 1.2 above.

External

5.4. Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)?

Yes, the data will be shared with the school(s) and State of residence reported on the FAFSA Application .

The external entities for disclosure include:

- Postsecondary institutions that the applicant designates on the application
- State agencies having agreements with the Secretary for the purposes of coordinating student aid
- Parents of a dependent applicant or an applicant spouse
- Freedom of Information Act (FOIA) Advice Disclosure, to the Department of Justice and Office of Management and Budget (OMB)
- Contract Disclosure
- Litigation and Alternative Dispute Resolution Disclosure
- Research Disclosure
- Congressional Member Disclosure
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Employment, Benefit, and Contracting Disclosure for decisions by the Department and for decisions by other public agencies and professional organizations
- Employee Grievances, Complaint or Conduct Disclosure
- Labor Organization Disclosure
- Disclosure to third parties through legally authorized Computer Matching Programs
- Disclosure to the Department of Justice (DOJ)
- Disclosure to the OMB for Federal Credit Reform Act (CRA) support
- Disclosure to third parties in the course of responding to breach of data

These disclosures are made on a case-by-case basis. CMAs have been authorized and approved prior to the sharing of data with another agency.

5.5. What information will be shared and with whom?

The information shared includes but is not limited to: SSN, DOB, legal addresses, first and last names, and email addresses. CPS shares information data with the following external entities:

- Internal Revenue Service (IRS)
- Social Security Administration (SSA)
- Veterans Administration (VA)
- Selective Service (SS)
- Department of Justice (DOJ)
- Department of Homeland Security (DHS)
- Office of Management and Budget (OMB)
- Department of Defense.

5.6. What is the purpose for sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

Personally identifiable information is shared to verify, validate, and authenticate a user's identity and this purpose aligns with the stated purpose in Question 1.

5.7. How is the information accessed and used by the external entity?

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

5.8. If the project is using the information for testing a system or for training/research purposes, what controls are in place to minimize the risk and protect the data?

Testing is conducted on a non-public facing test environment and all data used for testing is dummy data provided by the Social Security Administration. This data includes SSNs provided by the SSA that will never be distributed.

5.9. Does the system use "live" PII for the development or testing of another system? If so, please explain.

No

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?

The information sharing is pursuant to Computer Matching Agreements (CMA) or Memorandums of Understanding (MOU)s. CMAs have been authorized and approved prior to sharing data with other external entities, in accordance with the Privacy Act of 1974.

The Department may disclose information contained in a record in an individual's account without the consent of the individual under the routine uses listed under the Privacy Act of 1974, Computer Matching and Privacy Protection Act of 1989 and OMB Circular A-130.

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

Yes we do have limits on what we can re-dislose and it is outlined in the agreements that we our external partners. In the CMAs and MOU we define what we can disclose and how it will be used in determining aid.

6. Redress[4]

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

An individual receives a copy of the data that is submitted and using the FSAID the individual can access the application data

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 in FAFSA Corrections on the Web or they can work with the Financial Aid Administrator that 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 to assist individuals on the process of application submission and next steps.

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed onto Section 7. Safeguards.

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

The user receives an encrypted email with access to the data and results that were submitted on the application. In order for the user to see the data they must use the PAS (PIN) to retrieve the data stored on the Central Processing System Database. There is no way for the user to retrieve application data without the PAS.

7.3. 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, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

The confidentiality and integrity of information transmitted between the CPS and other external systems is protected by cryptographic mechanisms. Inbound and outbound CPS traffic is inspected using an industry standard intrusion protection system. All portable media, such as paper, backup tapes and CDs, are encrypted to otherwise physically secured, and accountability for the portable media during transport is maintained.
The Central Processing System is compliant with all relevant Federal security and privacy laws, regulations, standards and guidelines, as well as ED policies and procedures.

7.4. Is an Authority to Operate (ATO) required? Has one been granted?

Yes, CPS received its ATO on April 3, 2012.

7.5. Is the system able to provide an accounting of disclosures?

Yes

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 system owner along with the ISSO ensure that the data that is collected and stored on the system are following all the FISMA/NIST required controls and that all processes are documented according to the controls that are in the guidelines.

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

The privacy risks associated with the system is the database that houses all the applicant data that is submitted by the user. All necessary security controls are in place to ensure that the user's data is secure. The system is behind firewalls and all connections into the data center from external users submitting the data is encrypted as it is transmitted.