



Privacy Impact Assessment
For
Central Processing System (CPS)

Date:
March 25, 2013

Point of contact:
Calvin Whitaker
202-377-3045
Calvin.Whitaker@ed.gov

System Owner:
Keith Wilson
202-377-3591
Keith.Wilson@ed.gov

Author:
Calvin Whitaker
202-377-3045
Calvin.Whitaker@ed.gov

Office of
Federal Student Aid

U.S. Department of Education (DoED)
Expiration Date: October 2, 2009

1. System Information. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

The Central Processing System (CPS) is the automated system that processes all applications for Federal Student Aid (FSA), 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, developing and managing the mainframe eligibility determination system, providing Web-based applications and services, developing personal computer (PC) based financial aid software, printing and mailing eligibility documents and, supporting Participation Management (PM) for FSA Title IV programs.

CPS is comprises a number of technological and operational components. They include:

- Business Intelligence (BI) Tool
- Eligibility Determination
- FAA Access to CPS Online (FOTW)
- FAFSA on the Web
- FAFSA4caster
- Image and Data Capture (IDC)
- CPS Printing
- PIN Application
- Participation Management (PM)
- Institutional Student Information Record 9IRIS) Analysis (IA) Tool
- EDExpress Suite
- Student Authentication Network (STAN)
- IRS Datashare

Business Intelligence (BI) Tool is an analytically tool used for the Management Information System (MIS)/Business Objectives (BO) reporting. It provides a system for reporting on FSA Title IV system activity to FSA senior staff. The reports provide decision-making tools for monitoring and evaluating all FSA Title IV programs.

Eligibility Determination System (EDS) processes FSA applicant data and provides communications between students, postsecondary schools, and FSA office. The EDS must interact with various Federal and State Agencies, postsecondary institutions, private agencies serving the financial aid community, students and their families and, federal contractors. The EDS calculates the Expected Family Contribution (EFC), which postsecondary schools use to award student financial aid.

FAA Access to CPS Online consists of Student Inquiry, ISIR Requests Return of Title IV Funds (R2T4), ISIR Analysis (IA) Tool, and Application/Correction Entry. These functions assist Financial Aid Administrators (FAA) with administering the FSA programs.

FAFSA On The Web (FOTW) provides financial aid offices, students and other authorized agents with online access to the FAFSA. It provides the following major functionalities: electronic submissions of FAFSA applications, Renewal Applications (ROTW), FAFSA Corrections on the Web (COTW), and use of FAA Access to CPS Online.

FAFSA4caster provides early financial planning by estimating the Federal financial aid eligibility and a sample award package. FAFSA4caster calculates an estimated family contribution and the sample award package using the EFC formula and loan/grant limits based on current and projected information.

The Image and Data Capture (IDC) component scans paper financial aid documents (FAFSA's, SAR's and miscellaneous correspondence), data entry and, electronically transmits the data and related images to the CPS mainframe for processing.

The CPS Printing component print and mail all CPS related letters and correspondence such as PIN, PIN registration reject and reauthorization letters, SAR's, SAR Acknowledges, subsequent application, renewal reminder and, FAFSA4caster SSA match rejection letters to applicants.

The PIN Application components provides system authentication for access. Student applicants and their parents can view financial data or sign web applications electronically.

Participation Management (PM) consists of the PM Web and PM Mainframe. The PM Web allows users to enroll for electronic access to FSA data. Users gain access to CPS and NSLDS systems. The PM Mainframe processes the daily transmission of PIN requests, FAFSA transaction data and authentication to FAA Access to CPS.

ISIR Analysis (IA) Tool

EDEExpress Suite is a PC based developed software that provides for the Electronic Data Exchange (EDE) of FAFSA data between schools, State agencies and FSA.

Student Authentication Network (STAN) provides Web-based authentication using the PIN.

The FAFSA on the Web interfaces with the IRS system. The FAFSA on the Web also allows users to access relevant tax data from their filed Federal tax return. Users access FAFSA On The Web (FOTW) using their PIN. A user is authenticated by entering their PIN number, names (first and last), SSN, date of birth (DOB), address shown on tax return, tax year, and filing status. Upon authentication, the following information data will be available from the IRS system. Tax paper names (first and names), Tax year, SSN, Filing Status, Adjusted Gross Income (AGI), taxes paid, Type of tax return filed (1040, 1040A, etc), Number of exemptions claimed, Education credits, IRS deductions, Tax exempt interest income, Untaxed portion of pensions and Untaxed IRS distributions. Users will be able to print, save, copy and paste, or transfer the data directly into the online FAFSA.

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The Higher Education Act of 1965 Amended, Section 441 and 461 Title IV, Section 401.

3. **Characterization of the Information.** What elements of Personal Identifiable Information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number, etc.)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

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

A. Student (and spouse, if applicable) personal information

Personal information is collected and used to identify the student in the system and to determine if the student meets the eligibility requirements for Federal Student Aid (FSA). Personal information collected includes but is not limited to: SSN's, Names (first, last and middle initial), addresses, data of birth (DOB), telephone number, driver license number and State of issuance, email address, citizenship status and, marital status, month and year you got married. State of legal residence, date of legal resident if not born legally, male or female, if a male have you registered with Selective Service, high school diploma or its equivalent before you start college. Whether you will have your bachelor's degree before July 1 of the current year, and whether you have ever been convicted of possessing or selling illegal drugs while receiving FSA.

B. Dependency Status

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

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

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, investments, and the net value of businesses and/or investment farms.

D. Dependency Applicant's Parent Information

The information collected includes highest level of schooling completed, marital status, marital status date (month and date), SSN's , last name(s) and first name(s), dates of birth, email addresses, number in household supported by the parent(s), state of legal residence, date of parent(s) became legal residents, tax return information, untaxed income information, tax credit information, and asset net worth information.

The sources of information include student, teacher, employee and institutions. The information is collected by website, paper form and online form. This information is not used to link or cross reference multiple databases.

4. Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity. Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information is necessary to the mission of the Agency in order to comply with the HEA policies, regulations and statutes.

The privacy risks identified include the loss of data, stolen data, identity theft and misuse of data. These risks have been mitigated thru the use of PIN monitoring, access authentication and, security and intrusion detection software. All security vulnerabilities are identified are track and migrated thru the Operational Vulnerability Management System (OVMS).

5. Social Security Numbers - If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected.

Yes, SSN's are collected and used. The purpose of the collection of SSN's is to authenticate a user's identity.

The HEA Act of 1965 and Privacy Act of 1974 provide the disclosure information.

There are no alternatives when authentication is required by having a valid SSN. SSN's are matched with the Social Security Administration (SSA) and student are required validate the SSN and other information entered is correct. A valid SSN is required.

6. Uses of the Information. What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The information data is used to process all FAFSA applications calculates financial eligibility, identity and authenticates users and, provides Web-based services to students, families and postsecondary institutions.

Internal uses of the information include the exchange of data between FSA systems to include the National Student Loan Database System (NSLDS), Postsecondary Educational Participants System (PEPS), Student Aid Internet Gateway (SAIG) and, Common Origination Disbursement (COD). The exchange of information data with the internal systems provides program monitoring, student tracking, financial allocations, postsecondary institutional controls and, historical records and review.

External uses of the information include data sharing and identity matching and validation.

The external use of the information is to Web-based services to students, families lenders, and postsecondary institutions.

The Business Intelligence and ISIR Tools are used to analyze the data.

The publicly available information consists of non-personal identifiable data and this information can be obtained from postsecondary institutions. The information is used for public viewing, congressional and institutional tracking and monitoring, Title IV programs reviews and compliance. This information can be obtained thru the Freedom of Information Act (FOIA) request.

CPS uses the information from other Federal Agencies to perform applicant verification identity matching, viewing and/or importing data and, perform validation checks on names, addresses and date of birth.

7. Internal Sharing and Disclosure. Which internal DoED organizations will the information being shared? What information is shared? For what purpose is the information shared? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

The internal ED organizations this information will be shared with include National Student Loan Database System (NSLDS), Postsecondary Educational Participants System (PEPS), Student Aid Internet Gateway (SAIG) and, Common Origination Disbursement (COD).

The information shared is sensitive student level data as it pertains to students applying and receiving Title IV aid from FSA.

The purpose of the information sharing is to perform internal system monitoring, student tracking, payment allocation and historical records and review.

The privacy risks identified include the loss of data, stolen data, identity theft and misuse of data. These risks have been mitigated thru the use of PIN monitoring, access authentication and, security and intrusion detection

software. All security vulnerabilities are identified are track and migrated thru the Operational Vulnerability Management System (OVMS).

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.

8. External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement wit another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

CPS shares information data with the following external entities: Internal Revenue Service (IRS) Social Security Administration (SSA), Veterans Administration (VA), Department of Justice (DOJ), and the Office of Budget and Management (OMB).

Personally Identifiable information data is shared and the purpose of sharing this information is to verify, validate, and authenticate a user's identity. The information is shared electronically outside the Department over secure networks.

The information sharing is pursuant to CMA's and/or MOU's. CMA's have been authorized and approved prior to sharing data with other external entities.

Also, the Department may disclose information contained in a record in an individual's account under the routine uses listed under the Privacy Act of 1974, Privacy Protection ACT OF 1989 and OMB Circular A-130. The external entities for disclosures include the following;

Yes, 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, Privacy Protection Act of 1989 and OMB Circular A-130. The information shared includes but is not limited to: SSN, DOB, legal addresses, first and last names, and email addresses.

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 Consumer Reporting Agencies
Disclosure to third parties in the course of responding to breach of data
Disclosure to the Internal Revenue Service

These disclosures are made on a case by case basis. Computer Matching Agreements (CMA) have been authorized and approved prior to the sharing of data with another agency.

The privacy risks identified include the loss of data, stolen data, identity theft and misuse of data. These risks have been mitigated thru the use of PIN monitoring, access authentication and, security and intrusion detection software. All security vulnerabilities are identified are track and migrated thru the Operational Vulnerability Management System (OVMS).

9. **Notice.** Is a notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A notice is provided to the user prior to the collection of their information. The Privacy Act provides the individual the ability to access their account and the right to request an amendment of any inaccurate information in their record. The individual may request the information in their record from ED by calling 1-800-4FED-AID (1-800-433-3243). A full explanation of the individual's rights under the Privacy Act is set forth in the Department's Privacy regulations.

A system of record was created under the Privacy Act, 5U.S. C.522a as amended. It was published in the Federal Register on 12/27/1999 (69 FR 72400).

A link to the Privacy Act Statement can be found at: <http://www.ed.gov/notices/pai/pai-18-11-12.pdf>

10. **Web Addresses.** List the web addresses (known or planned that have a Privacy Notice.

<http://fafsaed.gov>

11. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a Certification and Accreditation (C&A) been completed? Is the system compliant with any federal security requirements? If so, which federal security requirements?

The security safeguards in place include but not limited to:

Audit Trails
Signed Rules of Behavior
OMB Clearances
Security Awareness Training
Vulnerability scanning

Change Management Process
Separation of Duties
Continuous Monitoring
Annual Auditing
System Authentication for access
System Firewalls
Intrusion Detection Software
System Required User Ids and Passwords

The CPS last Security Authorization (SA) was granted on July 25, 2008 and is compliant with all Federal Security requirements (OBM Circular A-130, NIST 800-53 and FISMA)

12. Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

Yes, a system of records has been created for this collection of information. Uses 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 FR30159). This notice was subsequently amended on December 1999 (64 FR 72047), March 2000 (65 FR 11294) and April 2001 (66 FR18758).

13. Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

Yes, CPS has a records retention and disposition schedule number from NARA. They are:

NARA Job No. NC-12-75-1 and NARA Job No. NC 12-80-2 and GRS 20.