Privacy Impact Assessment (PIA)

for the

Central Processing System (CPS)

January 6, 2023

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 Colon/Information System Security Officer
Contact Email: Nina.Colon@ed.gov

System Owner

Name/Title: Folajimi Ayodele/Information System Owner
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 operated by Federal Student Aid (FSA), an office within the U.S. Department of Education (Department). FSA uses CPS to process individual electronic or paper Free Application for Federal Student Aid (FAFSA) applications pursuant to Title IV of the Higher Education Act of 1965, as amended (Title IV). CPS is hosted on the Next Generation Data Center (NGDC) general support system (GSS). Upon receiving applications for aid from individuals, CPS calculates financial aid eligibility and notifies the applicant (through electronic or U.S. mail) of their eligibility to receive aid along with the types of aid available to them (i.e., loans and grants). The CPS sends Institutional Student Information Records (ISIRs) via FSA's Student Aid Internet Gateway (SAIG) system, which notifies institutions of higher education (IHEs) of the results of the eligibility calculation. The information contained in the ISIR is then used by IHEs to develop award packages which may include grants, loans, and school-based scholarships. Applicants receive award packages prior to enrollment to help them make decisions regarding attendance.

Key CPS system boundary components are as follows:

- Eligibility Determination is an internal application hosted on a mainframe system that calculates the student's Expected Family Contribution (EFC), which financial aid offices at IHEs use to assess how much aid should be awarded.
- FAA Access to CPS Online (FAA Access) is a web-based application that is used by financial aid administrators (FAAs) for managing Federal student aid programs at their schools through review of applicant information and processing of their requests for Federal aid. Only authorized users have access to the application, and access is managed by FSA's Access and Identify Management System (AIMS).
- CPS Services is a software solution that integrates with the studentaid.gov website, a component of Digital Customer Care (DCC), to allow applicants to electronically submit a FAFSA, check the status of a submitted FAFSA, and view or print processed results.
- SAIG Enrollment (Participation Management) is a web-based application used by IHEs to enroll for electronic access to several FSA systems, such as Common

Origination and Disbursement (COD), CPS, and National Student Loan Data System (NSLDS), used to manage and process financial data. A website is provided (fsawebenroll.ed.gov) for enrollment. Access is managed by FSA's AIMS.

- Business Intelligence (BI) tool is used by FSA staff for review of applicant submissions and CPS processing.
- CPS/SAIG Technical Help Desk is comprised of help desk agents that provide support to IHEs for issues regarding software, hardware configuration, and data processing.

In addition to the components above, CPS has tools that are used to support the CPS/SAIG Technical Help Desk. Functions used by the this help desk include:

- FAFSA Operations Tool (FOT) is accessed through the FAA Access website by CPS/SAIG Technical Help Desk agents to search for and view FAFSA applicant data in response to IHE callers' queries regarding application processing.
- CPS Business Services is an application that provides FSA Contact Center's customer relationship management (CRM) system and the Contact Center's Interactive Voice Response Unit (IVRU) to retrieve data from CPS to respond to callers' requests for application processing status.

CPS interacts with multiple FSA systems to gather information essential to the processing of Federal student aid applications. FAFSA data are supplied to CPS from the studentaid.gov website, a component of the DCC platform. CPS receives a daily file from the Postsecondary Education Participants System (PEPS) containing information on all IHEs that participate in Title IV programs. CPS retrieves information from the National Center for Education Statistics (NCES) to look up high school codes. CPS receives information from NSLDS to determine students' eligibility for Title IV financial aid. The Grant Recipient File is transmitted from COD to CPS via the SAIG network. CPS sends COD the email data record file (which contains records of applicants who will receive FAFSA related emails) and Demographic Data Exchange (DDE) file (which contains processing information for all transactions processed since the last file was transmitted) via the SAIG network. CPS receives a daily file of records from the Person Authentication Service (PAS) containing current and prospective student and parent identifying information such as social security numbers, names, and birth dates, which are sent to the U.S. Social Security Administration (SSA) for Social Security number (SSN) matching. This match determines the validity of student and parent SSNs. The Identity Verification Results Files – the outcome of a school's verifying and documenting a student's identity and high school completion status – are transmitted from CPS to the Enterprise Data Warehouse & Analytics (EDWA). EDWA is a repository for information about Federal student financial aid programs. All of these processes are conducted through the SAIG except for the FAFSA application, which is transmitted directly from studentaid.gov to CPS.

In addition to FAFSA information provided by applicants and other information provided by IHEs, additional data are provided by other Federal agencies to support application processing and eligibility verification. These include record match information from: U.S. Department of Defense (DOD) to identify applicants with parents/guardians who died during service in Iraq or Afghanistan after 2001; SSA to verify applicants' SSNs; U.S. Department of Justice (DOJ) to check whether an applicant is on drug abuse hold; U.S. Department of Homeland Security (DHS) to verify applicants' eligible non-citizen status; and U.S. Department of Veterans Affairs (VA) to verify applicants' veteran status. CPS also receives the SSA Death Master File, which is a list of all deceased individuals that SSA has on record, to validate the SSNs reported on the FAFSA and confirm eligibility. Information from these agencies is transmitted and received through the SAIG electronic file transfer system, with the exception of DHS, which uses a web-based secure file transfer protocol (SFTP).

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 from the FAFSA application, from IHEs, and from other Federal agencies. The PII is maintained in CPS to verify the identity of an applicant and/or the parents of a dependent applicant and in order to determine, process, and track financial aid 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

The PIA is being reviewed as part of the bi-annual review process.

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

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

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 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

The SORN, titled "Federal Student Aid Application File," 18-11-01, 84 FR 57856, was published in the Federal Register on October 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

[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

maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

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.

Department of Education Records Schedule No. 072 (DAA–0441–2013– 0002), FSA Application, Origination, and Disbursement Records (ED 072) is being amended, pending approval by NARA. Applicable Department records will not be destroyed until applicable NARA-approved amendments to ED 072 are in effect.

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.

Elements of PII collected and maintained by the system for parents and students applying for Title IV financial aid include:

- Full name
- SSN
- Driver’s license or State identification (ID) number
- Date of birth (DOB)
- Permanent Mailing address
- Telephone number
- Email addresses
- Citizenship status
- Veteran status
- Selective Service registration

- Drug abuse hold status
- Financial information including student/parent’s tax return filing status and type, adjusted gross income, income tax, earned income from work, savings/checking/cash account information, investments, untaxed income, any additional financial information, and loan disbursement information
- Student aid eligibility determinations
- Application processing status

Elements of PII collected and maintained by the system for IHE financial aid administrators include:

- First and last name
- Business address
- Business phone and fax numbers
- Email address
- Social Security number
- Date of birth
- Mother’s maiden name

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

Yes

The PII collected and maintained is the minimum amount required by CPS in order to develop award packages which may include grants, loans, and school-based scholarships. In addition, CPS utilizes the PII to uniquely identify individuals that apply for aid under the Title IV of the Higher Education Act and to track the status of their applications. Additionally, CPS is used by IHEs to view the application status of applicants and their parents which require the use of PII to uniquely identify them. If individuals do not provide the required PII, it may prevent the individuals’ student aid application from being submitted or processed and affect the possibility of receiving student aid.

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 on the FAFSA. Data are collected directly from the student/parent when they submit the FAFSA.

If the applicant is a current or previous borrower, their previous application information can be pulled from the NSLDS to assist in application completion.

Additional sources include the Federal agencies (DHS, DOD, DOJ, SSA, and VA) through which FSA conducts a computer matching program.

PII information is also collected from IHE officials for SAIG enrollment.

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 from studentaid.gov, a paper form, or via FAA Access by the school Financial Aid Administrator (FAA) working with the applicant and parent to complete the FAFSA application or make corrections on the students' application. Outside of the FAFSA process, PII is collected from IHE officials as destination point administrators for SAIG enrollment.

Information obtained from other Federal agencies is obtained through a computer matching program.

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 are submitted to the CPS from studentaid.gov, the data are run through system checks for data accuracy. For example, all data submitted to CPS are 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 are further validated through an applicant's use of the Internal Revenue Service's (IRS) Data Retrieval Tool (DRT).[4]

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

[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.

[4] The Data Retrieval Tool (DRT) is an online tool available as part of the FAFSA submission process. The DRT provides parents and students a way to transfer their income tax-return information directly into the FAFSA from the IRS.

basis ranging from daily to quarterly depending on the current Computer Matching Agreement (CMA).

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 also 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, PII is checked through various systems and processes to assist applicants in completing their application, ensure they provide accurate information, and ensure they 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

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 validating a user's identity. SSNs are also used to match records as part of computer matching programs with other Federal agencies for the purpose of determining eligibility for Federal student aid.

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

□ N/A

Alternatives to using SSNs have been considered but were determined to not be feasible given the design of systems at FSA and other Federal agencies, as well as the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA's data exchanges internally and externally rely on SSN to identify and track Federal student aid applications across different systems within and outside of the Department.

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 studentaid.gov 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

The FAFSA® Form Privacy Act Statement can be found embedded in the Privacy Policy for StudentAid.gov.

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?

Providing information to FSA is voluntary. However, individuals are required to complete a FAFSA if they want to apply for and receive Federal student aid. CPS is part of the student aid lifecycle, and once individuals provide information to FSA (submitted via the FAFSA or other FSA systems), the information will be maintained in CPS. After individuals provide the PII to FSA, they do not have the ability to decline to provide the PII or opt out from its use. Opportunities to decline to provide PII or opt out are at the initial point of collection on the FAFSA. If an individual declines to provide PII, that may prevent the individual's student aid application from being submitted or processed and affect the individual's eligibility and receipt of Federal student 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.

Yes

5.2 What PII will be shared and with whom?

□ N/A

A monthly file extract is provided to the Department's Office of the Inspector General's (OIG) Data Analytic System (ODAS), and includes data related to FAFSA awards. The This file extract contains applicant information derived of the FAFSA, which is used to support OIG field agents who are investigating applicants for potential fraud. PII contained within this data extract is listed in the response to question 3.1.

5.3 What is the purpose for sharing the specified PII with the specified internal organizations?

□ N/A

Records are shared with OIG to assist in identifying fraud. For more information on the uses of ODAS, please refer to the PIA for ODAS.

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.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

□ N/A

CPS shares student and parent full name, SSN, and DOB from FAFSA submissions with five other Federal agencies pursuant to CMAs: DHS, DOD, DOJ, SSA, and VA.

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

□ N/A

External data are provided by other Federal agencies pursuant to computer matching programs to support Federal student aid application processing and eligibility verification. These include computer matching information from:

- DOD to identify applicants with parents/guardians who died during service in Iraq or Afghanistan after 2001.
- SSA to verify applicants' SSNs. In addition, CPS receives the SSA Death Master File, which is a list of all deceased individuals that SSA has on record, to validate the SSNs reported on the FAFSA.
- DOJ to check whether an applicant is on drug abuse hold.
- DHS to verify applicants' eligible non-citizen status.
- VA to verify applicants' veteran status.

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

[5] 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.

Information from these agencies is transmitted and received through the SAIG electronic file transfer system, with the exception of DHS, which uses a web-based SFTP.

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 their FSA ID created through the FSA PAS that is created when the individual starts the FAFSA application. The user can log in to the studentaid.gov website with their credentials and access their application data and status. Users currently enrolled in an educational institution can also contact their FAAs for access to their records maintained in CPS.

Additionally, if an individual wishes to gain access to a record in this system, they may make a Privacy Act request through the Department's FOIA Office by completing the applicable request forms. Requests by an individual for access to a record must meet the requirements of the Department's Privacy Act regulations at 34 CFR 5b.5, including proof of identity.

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

Individual users may use their FSA ID to pull up their application using the FAFSA corrections function of the studentaid.gov website to make corrections to their application. CPS receives the corrected information once the correction application is submitted by the student/parent. In addition, users can work with the IHE FAA that can assist with correction to the application.

Additionally, if an individual wishes to contest or change the content of a record about themselves in the system of records, they can provide the System Manager with their name, DOB, SSN, and any other identifying information requested by the Department, while processing the request, to distinguish between individuals with the same name. The individual will need to identify the specific items to be changed and provide a justification for the change.

To contest the content of a FAFSA record for the current processing year (which begins on October 1 of the prior calendar year and continues for 21 months until June 30 of the following calendar year), an individual must send their request to the Department FOIA Office listed in question 6.1.

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

Once the applicant has submitted the FAFSA application and data have 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 instructions on the studentaid.gov 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 Authorization 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?

Access to the system is limited to authorized CPS program personnel and contractors responsible for administering the CPS program. Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing the CPS program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), CPS must receive a signed ATO from a designated FSA official. FISMA controls implemented by CPS are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

Physical safeguards include the staffing of security guards 24 hours a day, seven days a week, to perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest, access to records is strictly limited to those staff members trained in accordance with the Privacy Act and Automatic Data Processing (ADP) security procedures.

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 ATO. This process includes a tri-annual independent assessment of all required security and privacy controls and produces Plans of Actions and Milestones (POA&Ms) to ensure any deficiencies are remediated. CPS 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 ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, CPS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. 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 (LMM), which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as CMAs, information sharing agreements, and memoranda of understanding.

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 risks associated with CPS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

These risks are mitigated by granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission. Risks are also mitigated by updating security patches per the patch scheduling and updating devices' operating software, amongst other software. As referenced above, patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.

An additional risk to privacy is the possibility of 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 CMAs with other Federal agencies and validating returning applicant information against the PII currently maintained in NSLDS.