Privacy Impact Assessment (PIA)

for the

FAFSA Processing System (FPS)

December 14, 2023

Point of Contact

Contact Person: Corey Johnson
Title: Information System Owner (ISO)
Email: corey.johnson@ed.gov

System Owner

Name: Corey Johnson
Title: Information System Owner (ISO)
Principal Office: Federal Student Aid

Submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The Free Application for Federal Student Aid (FAFSA®) Processing System (FPS) will be operated by the Office of Federal Student Aid (FSA) within the U.S. Department of Education (Department) and will process individual electronic and paper FAFSA applications to determine student eligibility for Federal student aid pursuant to Title IV of the Higher Education Act of 1965 (Title IV) for Award Year (AY) 2024-25 and beyond. FPS will become operational in late 2023 and will completely replace the Central Processing System (CPS) on October 1, 2024. CPS will process FAFSA forms through AY 2023-24 and will then be decommissioned.

Upon receiving applications for Federal student aid, FPS will determine financial aid eligibility and notify applicants (through electronic or physical mail) of their eligibility to receive aid. FPS will also notify institutions of higher education (IHEs) of eligibility information via FSA's Student Aid Internet Gateway (SAIG) system. This eligibility information will be used by IHEs to create award packages which may include grants, loans, and school-based scholarships. Applicants will receive award packages prior to enrollment to help them make decisions regarding attendance.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

FPS will interact with multiple Department systems to gather information essential to the processing of Federal student aid applications to determine student eligibility for Title IV aid via an automated process as well as communicating data and outputs to other FSA systems for analysis and reporting. FAFSA data will be provided to FPS from studentaid.gov, a component of Digital Customer Care (DCC). FPS will receive a daily file from the Postsecondary Education Participants System (PEPS)/Partner Connect system containing information on all IHEs that participate in Title IV programs. FPS will retrieve information from the National Center for Educational Statistics (NCES) to

look up high school codes. FPS will receive information pertaining to applicants' prior or existing aid from the National Student Loan Data System (NSLDS). Grant recipient file and Federal Work Study (FWS) information will be received from the Common Origination and Disbursement (COD) system. FPS will match FAFSA data received from DCC with other information from the Student Aid Index (SAI), which is received from the Federal Tax Information Module (FTIM). The student's SAI will be included in the Institutional Student Information Records (ISIRs) used by financial aid offices at IHEs to determine how much aid should be awarded.

FPS will receive records from the Person Authentication System (PAS), which will be sent to the U.S. Social Security Administration (SSA) to verify individuals' identities using name, Social Security number (SSN), and date of birth (DOB). PAS sends information regarding individuals who do not have SSNs to TransUnion for identity verification; the result of this verification is stored in FPS.

Outcomes of verification and documentation of student identity and high school completion status will be transmitted to the Enterprise Data Management and Analytics Platform Services (EDMAPS) system, the repository for information about Federal student financial aid programs.

All data transfers listed above will be conducted through the SAIG except for the FAFSA application, which will be transmitted directly from studentaid.gov in the DCC system to FPS.

Other components of FPS include:

- Financial Aid Administrator (FAA) Access (faaaccess.ed.gov) is a web-based application that will assist FAAs with managing Federal student aid programs at their schools through review of applicant information and processing of their requests for Federal aid.
- FPS Client Services is a software solution that will receive FAFSAs submitted via studentaid.gov to allow applicants to check the status of a submitted FAFSA and view or print processed results.
- FAFSA Operations Tool (FOT) will be accessed through the FAA Access website by FPS/SAIG Help Desk agents to search for and view FAFSA applicant data in response to IHE callers' queries regarding application processing.

The FSA Information Center (FSAIC) Help Desk will also utilize FPS when responding to inquiries from applicants and other stakeholders. Functions used by the help desk include retrieval of transaction data, submission of limited corrections, and requests for duplicate student aid report reprints.

In addition to FAFSA information provided by applicants and information received from other FSA systems, external data will be provided by other Federal agencies to support application processing and eligibility verification. These include records matching information from:

- SSA: to verify identities using name, SSN, and DOB;
- U.S. Department of Justice (DOJ): to determine whether an applicant is on drug abuse hold;
- U.S. Department of Homeland Security (DHS): to verify applicants' eligible non-citizen status;
- U.S. Department of Veterans Affairs (VA): to verify applicants' veteran status; and
- U.S. Department of Commerce's (DOC) National Technical Information Service (NTIS) Death Master file: to identify deceased applicants.

Information from these agencies is transmitted and received through the SAIG electronic file transfer system, except for DHS, which uses a web-based secure file transfer protocol.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

FPS collects PII from the FAFSA application, from IHEs, and from other Federal agencies to allow FPS to calculate financial aid eligibility and notify the applicant (through electronic or physical mail) of their eligibility to receive aid along with the types of aid available to them (i.e., loans and grants). As a part of the eligibility determination process, PII is used to verify the identity of an individual (i.e., an aid applicant, parent, or contributor[2]) seeking to obtain login credentials (i.e., FSA ID).

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

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

[2] Contributor would include a spouse, or third-party nonpaid preparer.

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☐ N/A

The contractor's role is to develop and implement system changes, oversee operations, provide system maintenance as needed, and conduct annual close-out activities for the previous award year including but not limited to any other changes or updates as described in the contract.

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

Yes

☐ N/A

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, contact your program attorney.

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each 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 authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled "Aid Awareness and Application Processing," 18-11-21, 88 FR 39233, was last published in the Federal Register on June 15, 2023.

Records Management
If you do not know your records schedule, consult with your Records Liaison, or send an email to RMHelp@ed.gov

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

Department Records Schedule No. 072 (DAA–0441–2013– 0002), FSA Application, Origination, and Disbursement Records (ED 072). (The Department has proposed amendments to ED 072, for the National Archives and Records Administration's (NARA) consideration and approval. The Department will not destroy records covered by ED 072 until such amendments are in effect, as applicable.)

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

2.5. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

☒ Yes
☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☒ Gender or Sex
☒ City, State, or County of Birth	☒ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☒ Digital Signature ☒ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☒ Citizenship and/or Alien Registration Number (A-Number)	☒ Military Service	☒ Marital Status, Spouse, and/or Child Information (Specify below)
☒ Educational Background/Records	☐ Group/ Organization Membership	☒ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☒ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☒ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers

☐ License Plate Number	☒ File/Case ID Number	☒ Federal Student Aid Number
☒ Student ID Number	☐ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☐ Username/User ID	☐ Password	☒ IP Address
☒ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☒ Location Data	☒ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII: Financial information (i.e., asset and income information, tax filing status and return information, annual child support received), individual taxpayer identification number (ITIN), and pseudo-SSN (an identifier generated by the Department that is assigned to eligible non-citizens from specific countries from which the U.S. has a treaty allowing for provision of student aid to non-citizens.)

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☐ Federal Employees

Specify types of information collected from Federal employees:

☐ Federal Contractors

Specify types of information collected from Federal contractors:

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:[3]

From all below user types: IP address, MAC address, location data, and log data.

Applicants:

Name, address, SSN, ITIN (if applicable), DOB, telephone number, email address, citizenship status, alien registration number (A-number) (if applicable), country of birth, gender, race/ethnicity, marital status, status as a veteran, educational status, financial information (including asset and income information), and digital signature or hand signature.

Applicants' Spouses:

Name, DOB, SSN, ITIN (if applicable), address, marital status, personal telephone number, email address, digital or hand signature, tax filing status and return information, and annual child support received.

Parents:

Name, DOB, SSN, ITIN (if applicable), home address, personal telephone number, email address, digital or hand signature, marital status, educational background, tax filing status and return information, and annual child support received.

Parents' Spouses:

Name, DOB, SSN, ITIN (if applicable), home address, personal telephone number, personal email address, digital or hand signature, marital status, and tax filing status and return information.

Third-party Preparers:

[3] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

Name, SSN or employer identification number, telephone number, email address, name of company, and digital or hand signature.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

PII is collected from applicants, applicants' spouses, parents, parents' spouses, third-party preparers, IHEs, other Federal agencies, and other FSA systems.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, webpage, database)?

PII is collected via the FAFSA form, which can be completed in several ways, including directly through studentaid.gov, through a downloaded PDF, and through FAA Access by an IHE financial aid administrator assisting an applicant. PII is also obtained from other Federal agencies as part of the matching of data used to determine eligibility. PII is received from FSA systems other than DCC through SAIG.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

The PII collected and maintained is the minimum amount required by FPS to determine eligibility for Federal student aid and notify applicants (through electronic or physical mail) of their eligibility to receive aid. Name, SSN, DOB, and ITIN are used to uniquely identify applicants and contributors, including through matching their information with other Federal agencies, and track the status of their applications. Address, email address, and phone number are collected as contact information for applicants and contributors.

Financial information is required to calculate the SAI, which is used to determine the amount of aid an individual is eligible for. Gender, citizenship status, A-number (if applicable), marital status, veteran status, and educational status are required to be included in the FAFSA by the FAFSA Simplification Act for individuals to be eligible for Federal student aid.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

When the application data are submitted to FPS from studentaid.gov, the data are run through system checks for data accuracy. For example, all data submitted to FPS are validated against data in NSLDS if an applicant is a previous borrower. There are also content requirements for various fields, such as for SSNs, when an applicant completes the FAFSA form.

Additional checks on data integrity occur when PII is sent to match with other Federal agencies pursuant to the matching programs listed in Questions 1.2 and 5.6. Verification with these external databases is completed electronically. Responses are received after each data exchange. Responses can include rejections to unmatched PII.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

The collection of SSNs that are maintained in this system is authorized by 5 U.S.C. 301 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

SSNs are collected and used for the purpose of validating applicants' and contributors' identities. SSNs are also used to match aid applicant records contained in FPS against records contained in other FSA systems, records maintained by IHEs, and records maintained by other Federal agencies. SSNs are unique identifiers for individuals that remain consistent across all of these systems.

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

SSNs are required for all applicants and all contributors that possess an SSN to verify those individuals' identities and match records with other Federal agencies to determine eligibility for Federal student aid. If individuals decline to provide their SSN, that will prevent those individuals' student aid applications from being submitted or processed and they will be unable to receive student aid.

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

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

FPS uses alternatives to SSNs in limited cases where applicants or contributors do not possess SSNs. FPS assigns pseudo-SSNs to eligible non-citizen applicants

from countries with which the United States has a treaty allowing non-citizens to apply for student aid. Applicants using pseudo-SSNs and contributors that do not possess SSNs may submit ITINs as an alternative to SSNs for verification of Federal tax information.

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A Privacy Act Statement is provided before the applicant completes the FAFSA. This notice is provided both on the studentaid.gov website and the paper version of the FAFSA.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

☑ N/A

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

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

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

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. FPS 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 FPS. After individuals provide 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 will prevent the individual's student aid application from being submitted or processed and that individual will not be able to receive Federal student aid.

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

A monthly file extract is provided to the Department's Office of the Inspector General's (OIG) Data Analytic System (ODAS) that includes data related to FAFSA awards. This file extract contains applicant information derived from the FAFSA, which is used to support OIG field agents who are investigating applicants for potential fraud.

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☐ 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. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

FPS shares applicants', parents', and contributors' full name, SSN, and DOB from FAFSA submissions with the following Federal agencies pursuant to CMAs: SSA, DOJ, DHS, and VA. This information is also shared with DOC via MOU/interagency agreement (IAA).

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

External data are provided by other Federal agencies pursuant to computer matching programs (aside from the DOC NTIS sharing program, which is covered by a MOU/ IAA) to support Federal student aid application processing and eligibility verification. These data include information from:

- SSA: to verify individuals' identities.
- 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.
- DOC NTIS: to identify deceased applicants.

While FSA determines eligibility for Federal financial aid, actual financial aid packages are created and awarded by IHEs. Information pertaining to applicants is shared with IHEs listed on those applicants' FAFSAs to facilitate the creation of aid packages. In addition to the above matching programs, PAS sends information regarding individuals who do not have SSNs to TransUnion for identity verification; the result of this verification is stored in FPS.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

Title IV of the HEA (20 U.S.C. 1070 et seq.). The collection and sharing of SSNs of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

Information to and from external Federal agencies and IHEs is transmitted and received through SAIG, except for DHS, which uses a web-based secure file transfer protocol. All data transmission between FPS and the external systems is encrypted via TLS (FIPS-140 compliant) when in transit and at rest.

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☐ N/A

Yes

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

Yes

Information redisclosure is subject to restrictions as outlined in the respective CMAs or MOUs.

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Individual users may access their own application data using their FSA ID 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 FPS.

Additionally, if an individual wishes to gain access to a record in this system, they can contact the FPS system manager at the address listed in the SORN referenced in question 2.3. They must provide necessary particulars such as name, SSN, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name.

Alternatively, 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 individuals to correct or amend inaccurate or erroneous information?

Individual users may use their FSA ID to access their application and make corrections to their application using the FAFSA corrections function of the studentaid.gov website. FPS receives the corrected information once the correction application is submitted by the student/parent. In addition, users can request assistance from their IHE's FAA for corrections to application information.

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 FPS system manager, at the address listed in the SORN referenced in question 2.3, 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 written justification for the change.

Alternatively, 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.

Requests to amend a record must meet the requirements of the Department's Privacy Act regulations at 34 CFR 5b.7.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

Once the applicant has submitted the FAFSA application and their 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. Studentaid.gov also maintains instructions to assist individuals throughout the application process.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access to the system is limited to authorized FPS program personnel and contractors responsible for administering the FPS 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 FPS program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), FPS must receive a signed ATO from a designated FSA official. FISMA controls implemented by FPS 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 per day, seven days per week, that perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest and access to records is

strictly limited to those staff members trained in accordance with the Privacy Act of 1974, as amended.

8. Auditing and Accountability

8.1. How does the ISO 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, the FPS system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include 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 lifecycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as CMAs, Memorandums of Understanding (MOUs), and other information sharing agreements.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Continuous Diagnostics and Mitigation (CDM) scans are produced on a weekly basis to identify security and privacy vulnerabilities which are reviewed by the system owner, FSA Security Operations Center (SOC), Next Generation Data Center (NGDC) SOC and ISSO. In the review, system owners are notified of any findings that require action. FPS will also participate in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provide quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. FPS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner, in coordination with the ISSO and FSA Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. FPS will also

participate in annual assessments and audits as required, to ensure the effective safeguarding of PII.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

Privacy risks associated with FPS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII, and credentials 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.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, utilizing least privilege principles, masking SSNs, encrypting data in transmission, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by regularly updating security patches and device operating software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.

An additional privacy risk is the possibility of maintaining inaccurate information which could result in inaccurate eligibility determinations. This risk is mitigated by validating PII at various steps of the eligibility determination process. This is accomplished by entering into CMAs and MOUs with other Federal agencies and validating information received from these agencies against the PII currently maintained within FPS.