Privacy Impact Assessment (PIA)
for the

Postsecondary Education Participants System (PEPS)
November 3, 2022

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: Steven Ontiveros/Information System Security Officer
Contact Email: Steven.Ontiveros@ed.gov

System Owner

Name/Title: David Christie/System Owner
Principal Office: Office of 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 Postsecondary Education Participant System (PEPS) is a major application within the U.S. Department of Education (Department) Office of Federal Student Aid (FSA). PEPS is categorized as a moderate system and the data contained in the system are considered controlled unclassified information (CUI), including personally identifiable information (PII). PEPS is an Oracle-based client-server application. It is primarily used by the FSA Case Management team to manage and monitor school eligibility and certification for Title IV (part of the Higher Education Act of 1965) funds. The FSA Financial Partners team uses PEPS to manage and monitor lenders and guarantors.

PEPS stores a wide variety of school data to include data about school eligibility, certification, demographics, financial, review, audit, and cohort default rate data about schools. The data are stored in an Oracle database.

Postsecondary institutions use the PEPS Electronic Application (E-APP) to apply for designation as an eligible institution; to indicate initial participation, recertification, and reinstatement; to indicate a change in ownership of the institution; and to update a current approval of eligibility for participation. When institutions update a current approval of eligibility, such updates include, but are not limited to, name or address change, new location or program (e.g., adding a new program to the school, such as a Cybersecurity program), increased level of offering (e.g., adding upper-level degrees for programs already in place, such as a Master or PhD), change of officials (e.g., change of personnel), or mailing address for publications.

Information is initially collected from schools that submit application data through the E-APP system website. Information collected includes, but is not limited to, school name, owner (name), Taxpayer Identification Number (TIN), address, programs available, and officers (e.g., financial officer, board members). All E-APP users (a delegate designated by the school) log in to the system via web interface: https://eligcert.ed.gov.

PEPS collects names, email addresses, phone numbers, user IDs, and passwords for institution points of contact. For sole proprietorship institutions, the point of contact is the owner of the institution; for all other institutions, the point of contact is a representative designated by the school. PEPS also collects Social Security Numbers (SSNs) from owners of sole proprietorship institutions, but not from designated school representatives as the institution's employer identification number (EIN) is used instead. Federal employee and contractor work contact information, including name, email address, and phone number is collected for registration to access the system. Access is granted on a need-to-know basis. No other Federal employee/contractor information is required or stored within the system.

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

Information that is collected and processed enables the Department to effectively administer Title IV constituent eligibility, certification, and regulatory compliance. A postsecondary education institution must be approved by the Department for Title IV participation. A school must be accredited by a nationally recognized accrediting agency and authorized by the state in which it is located to be eligible for title IV programs.

When a school applies for Title IV eligibility, the school must provide information on their accrediting agencies and state authorizing agencies. The school must also provide information about the non-degree vocational programs and additional locations that they wish to be eligible, as well as information about their officials and owners. If they do not offer degree programs, the non-degree programs they provide must meet the Department's criteria for eligibility. The school must demonstrate that it is administratively capable and financially responsible. If the school meets the criteria, they are certified for appropriate Title IV FSA programs.

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

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

[1] 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

The PIA is being updated as part of the required biennial review.

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

Contractor

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

☐ N/A

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Higher Education Act of 1965, Title IV, as amended, (20 U.S.C. 1088, 1094, 1099c); the Debt Collection Improvement Act of 1996 (31 U.S.C. 7701).

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

The records are indexed by the name of the institution or organization and may be retrieved by the Office of Postsecondary Education Identifier (OPEID) of postsecondary educational institution, EIN of the postsecondary educational institution or entity; or the name or the TIN (generally the SSN) of the individual in the case of a sole proprietor institution.

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

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

The PEPS SORN Number is 83 FR 45912, entitled "Postsecondary Education Participants System (PEPS)" (18-11-09), published on September 11, 2018.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

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.

PEPS retains documents according to ED 074 FSA Guaranty Agency, Financial & Education Institution Eligibility, Compliance, Monitoring and Oversight Records (N1-441-09-15). Cut off records at the end of FY when financial action is completed. Destroy/delete 30 years after off. Records are stored at Iron Mountain. The archives that are older than 30 days are stored on a separate media and shipped offsite to Iron Mountain's storage facility.

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.

- First Name
- Last Name
- TIN
- SSN (if sole proprietorship)

- EIN
- Dun and Bradstreet (D&B) Number (DUN)[3]
- Email Address
- Phone Number
- School Address
- User IDs and Passwords

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

Yes

PEPS collects only the minimum information necessary. Information collected by PEPS is needed to vet postsecondary institutions that apply for designation as an eligible institution; to indicate initial participation, recertification, and reinstatement; to indicate a change in ownership of the institution; and to update a current approval of eligibility for participation. The institution's TINs/EINs or SSNs (if sole proprietorship) are collected and used by PEPS through E-APP to identify the individual institutions and ensure that FSA can match an institution's records across FSA enterprise systems. This is a business requirement and there are no other alternatives available without storing the TIN/EIN or SSN.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

PII is collected from individuals (sole proprietorship) and schools.

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

PII is collected electronically through use of the following web page: https://eligcert.ed.gov.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

[3] For more information, please see: What is a D-U-N-S Number? (dnb.com)
[4] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

PII is validated through the D&B website. Any debarment from the government triggers an invalidation status from the School Participation Division within FSA. The school's owner submits their TIN when submitting their application. The provided TIN is checked against the school's D&B account to see if they have been barred from doing business with the Federal Government. The schools will either use their SSN if they are a sole proprietorship, or they will enter their EIN/TIN on their D&B account and their E-APP account.

In addition, PEPS stores school data to include data about school eligibility, certification, demographics, financial, review, audit, and cohort default rate data about schools.

Use

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

PII is collected to manage and monitor school eligibility and certification for Title IV (part of the Higher Education Act of 1965) funds. The FSA Financial Partners team uses PEPS to manage and monitor lenders and guarantors. The institution's TINs/EINs or SSNs (if sole proprietorship) are collected and used by PEPS through E-APP to identify the individual institutions and to ensure that FSA can match an institution's records across FSA enterprise systems. This is a business requirement and there are no other alternatives available without storing the TIN/EIN or SSN.

For school officials, full name, phone numbers, and email addresses are recorded for contact purposes. Login credentials are needed to allow for school officials to log in to the E-APP system.

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, 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. Please note: the Application requests the Social Security numbers

(SSNs) of the owners of the institution. The SSNs are used to determine institutional eligibility and to verify identities.

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

The institution's TINs/EINs (which may be an SSN in the case of a sole proprietorship) are collected and used by PEPS through E-APP to identify the individual institutions and to ensure that FSA can match an institution's records across FSA enterprise systems. This is a business requirement and there are no other alternatives available without storing the TIN/EIN or SSN.

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

☐ N/A

While alternatives were considered, the TIN/EIN and SSN (in the case of sole proprietorships) are required to uniquely identify institutions across the FSA enterprise and with D&B to identify debarment from the government, as these are the unique identifiers associated with institutions.

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. A Privacy Act Statement is located on the E-APP website: https://eligcert.ed.gov/ows-doc/intro.htm#privacy.
b. A Privacy Policy and Statement is also provided in the PEPS user access form and agreed on by the user prior to granting access to PEPS and E-APP.

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

E-APP website:

Authorities: The following authorities authorize the collection of this information: Higher Education Act and Title 31 as amended by Section 31001 of Public Law 104-134 of the Debt Collection Improvement Act of 1996. Section 498A(a)(3) of the HEA requires the Secretary to establish a central database of information on institutional accreditation, eligibility, and certification that includes all information available to the Department. Section 498A(c) instructs the Secretary to make this information available to all institutions of higher education, guaranty agencies, states, and other organizations participating in the programs authorized under Title IV of the HEA.

Please note: the Application requests the Social Security numbers (SSNs) of the owners of the institution. The SSNs are used to determine institutional eligibility and to verify identities. The SSNs are collected under the authority of the Debt Collection Improvement Act of 1996, Pub. L. 104-134. This act requires Federal agencies to secure the TIN (the Social Security Number, for individuals) of persons "doing business with the agency," a term that includes being "in a relationship with the agency that may give rise to a receivable due that agency." 31 U.S.C. §7701(c)(1), (2)(E). Due to security concerns, U.S. Department of Education is not collecting SSNs on this website at this time. Instead, if applicable, you must submit your SSNs to U.S. Department of Education by writing them on Section M of the application and including it with your supporting documents.

Information Collected: We only collect information that we need to determine if the institution is eligible, and if applicable, certified to participate in the Title IV, HEA programs. Information collected includes, but is not limited to, name, work title/role school name, owner (name), tax ID number (TIN), Dun and Bradstreet (D&B) Number (DUN), address, programs available, officers (e.g., financial officer, board members), and contact information (such as name, email address, phone number).

Purpose: Postsecondary institutions use the E-APP to apply for designation as an eligible institution, initial participation, recertification, reinstatement, or continued approval after a change in ownership, or to update a current approval. Updates

include changes such as, but not limited to, name or address change, new location or program, increased level of offering, change of officials, or mailing address for publications. This includes information about the school's name, address, locations, programs, officials, authorizing agencies, owners, and servicers.

Disclosures: Information is validated through the Dun & Bradstreet (D&B) website. The provided TIN is checked against the school's D&B account to identify if the school has been barred from doing business with the Federal Government.

Consequences of Failure to Provide information: If you chose not to submit an Application for Approval to Participate in Federal Student Financial Aid Programs, the institution cannot be determined to be eligible or continued to be eligible for the Title IV FSA programs.

No cookies or other tracking technology are used on the website. If you decide to send us an electronic mail message (email), the message will usually contain our return email address. If you include personally identifiable information in your email because you want us to address issues specific to your situation, we may use that information in responding to your request. Please send only information necessary to help us process your application.

Please contact us at U. S. Department of Education, Federal Student Aid, 830 First Street, NE, Washington, DC 20002-5402, or call 1-800 872-5327, or email us at customerservice@inet.ed.gov to ask any questions regarding our Privacy Policy and our Privacy Act Statement.

PEPS user access form:

The information collected on this form is authorized by the Higher Education Act of 1965, as amended, and the Federal Information Security Modernization Act of 2014. This information is collected so PEPS staff can ensure you are a legitimate requestor of access to PEPS and to provide you with the appropriate level of access to PEPS. This information may be furnished to appropriate Federal, state, and/or local law enforcement authorities, and/or other third parties as authorized by law, in accordance with the routine uses described in the Postsecondary Education Participants System (PEPS) System of Records notice (SORN; number 18-11-09). A complete copy of the PEPS SORN is available here.

This information collection is voluntary on your part; however, if you do not provide the information requested on this form, you will not be provided access to PEPS.

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?

Schools have the opportunity to decline to provide the information; however, providing certain information is required to determine whether or not a school is eligible or will continue to be eligible for the Title IV FSA programs.

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

The PEPS daily school file is processed Monday-Friday excluding Federal holidays and is copied to a directory on the PEPS Unix Database Server. For the Department's Grants Management System (G5), PEPS sends the daily school file using Secure File Transfer Protocol (SFTP) for the purposes of grants pre-award processing, to include accounting for the grant application submission and review process. Grant processing encompasses grant award notification, funding, and grant payment processing.

5.2. What PII will be shared and with whom?

☐ N/A

The specific information that will be shared with the G5 system within the Daily School File includes:

- First Name
- Last Name
- Institution TIN and EIN
- SSN (if sole proprietorship)

- DUN
- Email Address
- Phone Number

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

☐ N/A

PEPS sends the daily school file to the G5 system, providing information related to if a school or institution is still in good standing, to maintain compliance with Title IV regulations for funding. G5 uses the information provided by PEPS for the purposes of grants pre-award processing, to include accounting for the grant application submission and review process. Grant processing encompasses grant award notification, funding, and grant payment processing.

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

PII is shared and validated through the D&B website. Any debarment from the government triggers an invalidation status from the School Participation Division within FSA. The provided TIN/EIN or SSN (if a sole proprietorship) are checked against the school's D&B account to see if they have been barred from doing business with the Federal Government.

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

The school's TIN/EIN or SSN (if a sole proprietorship) are checked against the school's D&B account to see if they have been barred from doing business with the Federal Government.

[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.

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

☐ N/A

FSA checks information against the D&B website to determine if a school has been debarred from government business.

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

TINs/EINs or SSNs (if a sole proprietorship) are inputted into the D&B website to search a school's debarment status.

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

No

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

☐ N/A

No

Information is validated through the D&B website. The provided TIN is checked against the school's D&B account to identify if the school has been barred from doing business with the Federal Government. Information used to validate schools is already maintained within D&B, therefore information is matched with D&B and ultimately is not stored

within the D&B environment. For further information on how D&B may share information to third parties, please refer to their privacy policy.

6. Redress

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

If an individual wishes to gain access to any record in the system of records, they must contact the system manager at the address listed in the above SORN. They must provide the necessary particulars of their name, SSN, and any other identifying information requested by the Department, while processing the request, to distinguish between individuals with the same name. The individual must meet the requirements in 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?

If an individual wishes to contest the content of a record in this system, they must contact the system manager at the address listed in the above SORN. The request to amend must be made in writing and addressed to the system manager at the address provided above with the necessary particulars of their name, SSN, and any other identifying information requested by the Department, while processing the request, to distinguish between individuals with the same name. The request must identify the particular record within the PEPS that they wish to have changed, state whether they wish to have the record amended, corrected, or deleted, and explain the reasons why they wish to have the record changed. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

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

Schools can contact their respective FSA School Participation Division (broken out by regions) to correct any inaccurate information. This information is available on the FSA Partners website.

7. Safeguards

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

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

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

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

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), PEPS must receive a signed ATO from a designated FSA official. FISMA controls implemented by PEPS 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.

PEPS 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. PEPS 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. PEPS 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, PEPS 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.

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?

Privacy risks associated with PEPS 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.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, 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 updating security patches per the patch scheduling and updating devices' operating software, amongst other 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.