Privacy Impact Assessment (PIA)

for the

Ez-Audit (EZAUDIT)

September 2, 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 (ISSO)
Contact Email: Steven.Ontiveros@ed.gov

System Owner

Name/Title: David Christie/Information System Owner
Principal Office: Federal Student Aid (FSA)

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 Ez-Audit System (EZAUDIT) is comprised of a public-facing website and backend database that provides educational institutions that participate in the Title IV Federal student aid program (authorized by the Higher Education Act of 1965) with a paperless single point of receipt for financial statements and compliance audits via a web-based application. The U.S. Department of Education (Department) accesses this system to review the financial documents the schools and third-party servicers submit as part of their compliance review. This review ensures the schools are distributing student loans in compliance with Title IV.

There are two types of users: Department employees/contractors and the individuals designated by Title IV institutions to submit the required documents. Users log onto EZAUDIT by providing a valid user ID and password. To create these access privileges, EZAUDIT collects users' name, work email address, office phone number and office fax number. Users with the proper permissions can submit financial statements and compliance audits through the system. The user's submission is sent to and stored in the EZAUDIT database.

Department users can request access to the system by contacting the EZAUDIT help desk with a confirmation email from their supervisor, or via a contract officer representative (COR) requesting an account on their behalf. Once approved, the Department user will receive an email with their user ID and temporary password that the user will update.

For institution representatives, the EZAUDIT system administrator receives an official PDF from the school or third-party servicer providing approval for the named representative within the letter to obtain an account. Third-party servicers are companies that specialize in performing financial work for institutions; they can upload audit-required documents to the system similar to a tax preparer. These PDFs are stored within the system. To create accounts for institution representatives, the system collects name, email address, phone number, and fax number. Upon approval, the institution representative will receive two separate emails: one with their user ID and the other with their temporary password that the user will update. The complete process can also be found on the EZAUDIT website.

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

PII is collected to create these accounts for privileged users. EZAUDIT collects users' names, email addresses, and phone numbers. Users with the proper permissions can submit financial statements and compliance audits through the system.

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?

New PIA

During a review of EZAUDIT, it was determined that a PIA is required for this system.

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.

EZAUDIT is authorized by Title IV of the Higher Education Act of 1965, as amended (Title IV, HEA Programs).

[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

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?

No

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

2.2.2. 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

Information is retrieved by school-specific information such as institution name, city, state, Office of Postsecondary Education ID (OPEID), etc. Information is not retrieved by name or other personal identifier.

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.

The applicable Department records schedule is ED 74: FSA Guaranty Agency, Financial & Education Institution Eligibility, Compliance, Monitoring and Oversight Records (N1-441-09-015).

This system allows entities that participate in Title IV programs to submit financial statements and compliance audits electronically and facilitates the processing of these through the School Eligibility Channel (SEC). The Department collects, copies, screens,

[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

disseminates, reviews, and files financial statements and compliance audits from proprietary, non-profit, and public entities that participate in Title IV programs. TEMPORARY cut off at the end of the fiscal year in which the final action is completed. Destroy/delete 30 years after cut off.

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.

EZAUDIT collects the following during user registration:

- External users:
  - First name, last name, work email address, office phone number and office fax number, username, password.
- Department users:
  - First name, last name, work email address, username, password.

During the compliance audit and financial statement submission process on the website, the following submission contact information is collected from the school's designated user:

- First name, last name, work email address, office phone number.

A Federal Student Aid user can update the auditor information through the website with reference to the auditor information on their letterhead as displayed in the pdf attached to the electronic submission. The auditor information collected/updated during this process is:

- Name of auditor/auditing firm, the Tax Identification Number (TIN) of the auditor/auditing firm, office address (street, city, state, province, country, postal code), office phone number, and office fax number.

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 EZAUDIT to establish user accounts for the purpose of collecting submission for financial statements and compliance audit documentation from educational institutions that participate in the Title IV Federal student aid program. The Department's review ensures the schools are distributing student loans in compliance with Title IV.

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

Schools' and third-party servicers' institution representatives (designated by the school/third-party servicers for managing the school's access to the EZAUDIT)

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

As stated within the EZAUDIT registration instructions, institutions are required to prepare a letter on company letterhead that contains the following information:

- First and last name of appropriate person in authority (e.g., President/CEO)
- Signature of person named above
- First and last name of EZAUDIT Institution Administrator
- Signature of designated EZAUDIT Institution Administrator
- Email address of EZAUDIT Institution Administrator
- Phone number and extension (if applicable) of EZAUDIT Institution Administrator
- Fax number of EZAUDIT Institution Administrator

Once the letter has been created, institutions are requested to submit their registration request via email to fsaezaudit@ed.gov.

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?

Individuals provide information when they contact the Department. Validation relies on the individual providing correct contact information for the Department in order to create an account. Quarterly checks occur to validate user accounts. Emails are sent out to active accounts requesting the need for continued use. Those who do not respond have their accounts deactivated.

[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.

Use

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

PII is used to create accounts for privileged users from educational institutions that participate in the Title IV Federal student aid program. Users with the proper permissions can submit financial statements and compliance audit documentation through the system, as required by the Department.

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.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

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

☑ N/A

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.

Notice is provided to individuals accessing EZAUDIT on the login webpage. In addition, notice of how information is handled once submitted to the Department is provided through the publication of this PIA.

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

Link to the EZAUDIT login webpage: eZ-Audit Web Site (ed.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?

The information collected directly from individuals is strictly voluntary, giving individuals the option to decline or opt out. Individuals can email webmaster@fsa.ed.gov with questions. Once they have been approved for access, they can mail a letter or email fsaezaudit@ed.gov if they would like to opt out later.

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

First name, last name, work email address, office phone number and office fax number will be shared with the Postsecondary Educational Participants System (PEPS).

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

□ N/A

FSA uses the information that is provided in other ways to further FSA's mission of maintaining stability and public confidence in the nation's banking system. This sharing allows FSA to continue to manage and monitor school eligibility and certification for Title IV (part of the Higher Education Act of 1965) funds.

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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

[4] 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.

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☑ N/A

Click here to enter text.

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

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

If an individual requires access to their information maintained in EZAUDIT, they may obtain access by logging into their online account through the website. The individual is able to access their information on the "My Profile" page.

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

The individual is able to update their information on the "My Profile" page by logging into their account within the system. The individual can also send an email to the fsaezaudit@ed.gov requesting their information to be updated.

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

The system informs the users of the procedures for correcting their information in the following ways:

- Within the initial registration confirmation email. Once a registration request is processed, the individual will receive an email that contains the EZAUDIT username, instructions for accessing the EZAUDIT website and procedures for correcting inaccurate information.

- During the quarterly inactive user validation emails. These quarterly emails contain procedures for correcting any inaccurate information.

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 EZAUDIT program personnel and contractors responsible for administering the EZAUDIT 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 EZAUDIT program.

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

EZAUDIT 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. EZAUDIT 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. EZAUDIT 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.

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 EZAUDIT 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 compromised credentials, embarrassment, or malicious compromise of the confidentiality and integrity of the individual's personal information. 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 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.