Privacy Impact Assessment
for
eZ-Audit

Date:
February 25, 2010

Point of contact:
Asha Gupta
202-377-3939
Asha.Gupta@ed.gov

System Owner:
Ti Baker
202 377-3156
Ti.Baker@ed.gov

Author:
Jennifer Quansah
703 891 6921
Jquansah@2020llc.com

Office of
Federal Student Aid
U.S. Department of Education (DoED)

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

eZ-Audit is a Major Application (MA) within Federal Student Aid's IT infrastructure. This system provides a paperless point of receipt for financial statements and compliance audits received from schools that participate in Title IV funding.

Users log onto the eZ-Audit System by providing a valid user ID and password via a web interface. The system stores users' access privileges, which are various combinations of view, read, and write. Users with the proper permissions are allowed to submit the financial statements and compliance audits over the Web. The user's submission is sent to and stored in the eZ-Audit database. Users include Federal Student Aid Case teams and the individuals designated by Title IV institutions to perform submission of the required documents.

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

The Federal Register is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents.

eZ-Audit was granted legal authority to collect data on May 16, 2003 as documented in the Federal Registrar Volume 68, Number 95 Notices (pages 26586-26587) with the following action:
"Notice implementing a new electronic process(eZ-Audit) for submitting compliance and financial statement audits."

The summary of this authority includes the following details: SUMMARY: The Secretary gives notice that on June 16, 2003, the Department will fully implement the eZ-Audit process under which an institution that participates, or seeks to participate, in the Federal student aid programs submits its compliance and financial statement audit information electronically. The Federal student aid programs are authorized under Title IV of the Higher Education Act of 1965, as amended (Title IV, HEA Programs). This notice applies to any compliance or financial statement audits that an institution is required to submit under 34 CFR 600.20(a) or (b) to begin or continue participating in the Title IV, HEA Programs, any financial statement audits required for an institution that undergoes a change in ownership resulting in a change in control as provided under 34 CFR 600.20(g), any compliance and financial statement audits that an institution is required to submit annually under 34 CFR 668.23, and any compliance and financial statement audits required of an institution that ceases to participate in the Title IV, HEA Programs as provided under 34 CFR 668.26(b).

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

During the user registration process which occurs in paper form and/or through the website, the following eZ-Audit user information is collected from the school's designated user:

First name, Last name, office email address, office phone number and office fax number.
This information is not linked with other databases. 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: Name, Office Email and 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. This information is transferred to the PEPS system.

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

This information enables Federal Student Aid to manage its trading partner eligibility, enrollment, participation, and oversight processes to include, schools and auditors as they administer Title IV Financial Aid for Students.

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

This system does not collect or use social security numbers.

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

This information enables the Department of Education to effectively administer Title IV constituent eligibility, certification, and regulatory compliance. A Postsecondary educational institution must be approved by the Department of Education for Title IV participation. When a school applies for Title IV 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 – Federal Pell Grant, Federal Perkins Loan, Federal Supplement Educational Opportunity grants, Federal Work-Study, Federal Family Education Loan (FFEL), and Federal Direct Loan. At the end of each year of participation as school must submit its financial statements and compliance audits. When a school finishes its participation in Title IV programs, it must submit a close-out audit for the final period of participation.

The information is used to contact institutions, send incomplete, delinquent and reminder notifications.

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

The PEPS application has read-only access to the eZ-Audit tables to present the information required in the PEPS application. To facilitate the consistent data approach, data cannot be updated via PEPS and PEPS will not hold any persistent data any information in its own database. PEPS writes any required logic to reference eZ-Audit data in a read-only manner.

The PEPS application requires access to eZ-Audit data for:

- Reporting (Consolidated and other)
- Forms / Screens pre-population
- Data Access for non-eZ-Audit users (OGC, OPE, Guaranty Agencies, State Licensors, Crediting Agencies, and other Dept. Of Ed Users)

8. External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU)

or other type of approved sharing agreement wit another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The information is not shared with any other agency.

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

This notice is provided at the eZ-Audit public website home page:

"WARNING:
This is a Department of Education computer system. Department of Education computer systems are provided for the processing of Official U.S. Government information only. All data contained on Department of Education computer systems is owned by the Department of Education and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on Department of Education computer systems. Unauthorized use of this system is a violation of Federal law and can be punished with fines or imprisonment (P.L. 99-474). "USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.

Information Collected from You:

You may decide to send FSA information, including personally identifying information. The information you supply - whether through a secure Web form, a standard Web form, or by sending an electronic mail message - is maintained by FSA for the purpose of processing your request or inquiry. FSA also uses the information you supply in other ways to further FSA's mission of maintaining stability and public confidence in the nation's banking system. Various employees of FSA may see the information you submit in the course of their official duties. The information may also be shared by FSA with third parties to advance the purpose for which you provide the information, including other federal or state government agencies. For example, if you file a complaint, it may be sent to a financial institution for action, or information may be supplied to the Department of Justice in the event it appears that federal criminal statutes have been violated by an entity you are reporting to FSA. The primary use of personally identifying information will be to enable the government to contact you in the event we have questions regarding the information you have reported. If you are concerned about how information about you may have been used in connection with this web site, or you have questions about the FSA's privacy policy and information practices you should e-mail us at webmaster@fsa.ed.gov. Electronic mail is not necessarily secure. You are advised to be cautious when sending electronic mail containing sensitive, confidential information. As an alternative, we advise users to give consideration to using postal mail. "

eZ-Audit users can decide not to submit any information and not continue to use the system.

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

The privacy notice, as shown above, is displayed on the eZ-Audit public website home page:
https://ezaudit.ed.gov/EZWebApp/default.do

11. Security. What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a Certification and

Accreditation (C&A) been completed? Is the system compliant with any federal security requirements? If so, which federal security requirements?

The information will be secured following the guidance of OMB Circular A-130, "Management of Federal Information Resources, "Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987." The system security plan details the security requirements and describes the security controls that are in place to meet those requirements.

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

A system of record as defined by the Privacy Act is not being created and the reporting requirements of OMB Circular A-130 does not apply.

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

These records are covered by 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 final action is completed. Destroy/delete 30 years after cut off.

Certifying Officials Signatures.

Senior Program Official — Date: 3/2/10

Computer Security Officer — Date: 3/5/10

For systems that collect, maintain and or transfer SSNs:

Assistant Secretary or equivalent — Date

Privacy Advocate — Date: 3/26/10