Privacy Impact Assessment for the

Postsecondary Education Participate System (PEPS)

Date
March 17, 2008

Contact Point
System Owner: Molly Wyatt
Author: Nita Washington (System Security Officer)

Federal Student Aid
U.S. Department of Education

1. **What information will be collected for the system?**

   Information of individual users collected
   Full Name
   Work Phone
   Region number and State

2. **Why is this information being collected?**

   (1) 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.

3. **How will FSA use this information?**

   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. 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 of Education'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 SFA programs - Federal Pell Grant, Federal Perkins Loan, Federal Supplement Educational Opportunity grants, Federal Work-Study, Federal Family Education Loan (FFEL), and Federal Direct Loan.

4. **Will this information be shared with any other agency? If so, with which agency or agencies?**

   This information is not shared with any other agency.

5. **Describe the notice or opportunities for consent that will be/or are provided to individuals about what information is collected and how that information is shared with others organizations.**

   The following is posted on the application's login 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.

6. **How will the information be secured?**

The Department of Education develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

All policy and procedures may be found on ED's internal website at: http://connectED.

Federal Student Aid provides comments on departmental policy and procedures through the department's Administrative Communications System (ACS) process.

PEPS reviews: account management processes, account establishment, activation, modification, disabling, and removal. PEPS also reviews periodically for account reviews and disablement.

The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

Access to sensitive materials, such as user security forms is maintained by the SSO. This data is stored in locked and protected files.

In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

7. Is a system of records being created or updated with the collection of this information?

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

8. List the web addresses (known or planned) that will have a Privacy Notice.

Exempt: PEPS is not a publicly accessible system, and is accessible only by authorized internal users, and external partners.

As the system is not publicly accessible, and does not collect any personally identifiable information directly from any public end user, PEPS is exempt from placing a privacy notice on the website. In accordance with OMB Memo M-03-22, Attachment A, Section III (C), dated September 26, 2003, PEPS is excluded as the guidance does not apply to "agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees)."