Privacy Impact Assessment for the Direct Loan Consolidation System (DLCS)

Date
June 10, 2008

Contact Point
System Owner: Jana Hernandes
Business Owner: Mike Murray
Primary Application Owner: Denise Leifeste
Author: Gregory Plenty (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
Address
SSN (required)
Phone
Email
Employment Information

2. Why is this information being collected?

(1) This information is collected to complete official Government business related to the administration of the Direct Loan Program.

3. How will FSA use this information?

The Direct Loan Consolidation System (DLCS) supports borrowers' requests for loan consolidations and for the disbursement of loan funds. The DLCS assists in tracking information pertinent to the borrower, as well as loan disbursement information during the life of a loan.

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

Yes. This information will be shared with the following agencies and/or companies:

- Wachovia Bank
- Surveyor (Online Application)
- U.S. Department of Education (EDNET)
- Computer Sciences Corporation (CSC)
- Affiliated Computer Services (ACS)
- Direct Loan Consolidation (DLC) Image Repository
- Internal FSA Interfaces
    - Collections (DMCS)
    - National Student Loan Database (NSLDS)
    - Financial Management Systems (FMS)
    - Student Aid Gateway (SAIG)
    - Grants Administration and Payment System (GAPS)

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.

There is no Privacy Notice on DLCS; however, there is a Warning Banner that speaks to User Monitoring. The banner states the following:

"…Use of the Network is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the Network expressly consents to such monitoring and recording. Be advised if possible criminal activity is detected, system records, along with certain personal information may be provided to law enforcement officials…"

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.

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

The application IDs are reviewed by the SSO quarterly. The SSO provides a list of current users to business POCs and requests them to verify who has left the project or no longer needs access to the application. The SSO will remove access as appropriate.
Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. 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.

The information is 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." In addition, CSB is currently re-writing the System Security Plan (SSP) that details the security requirements and describes the security controls that are in place to meet those requirements. A certification and accreditation process in accordance with the National Institute of Standards & Technology (NIST) "Guide for the Security Certification and Accreditation of Federal Information Systems" will validate our security controls.

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

A "System of Records" was created for the Common Services for Borrowers (CSB) Contract. DLCS is working under this "System of Records."

The "System of Records" was published in the Federal Register (Volume 71, Number 14/Monday, January 23, 2006/Notices).

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

http://loanconsolidation.ed.gov/