Privacy Impact Assessment for the Electronic Campus-Based System (eCB)

Date
August 30, 2005

Contact Point
System Owner: William Leith
Author: Tammy Connelly (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
Phone
Email
Financial Information (as it pertains to the campus-based programs) from schools who participate in the campus-based programs

2. Why is this information being collected?

(1) Contact information for schools is collected so FSA knows whom to contact for answers to questions regarding data submitted on the FISAP and to provide information regarding campus-based funding.

(2) Contact information for state agencies is collected so FSA, schools, lenders, and borrowers know whom to contact for answers to questions regarding the listing of eligible low-income schools.

(3) Contact information for Perkins Loan recipients that are delinquent in repaying their loans is collected to allow FSA to assist schools in their collection efforts.

(4) Financial information is collected to assist FSA in the proper management of the campus-based programs.

3. How will FSA use this information?

(1) Contact information for schools will be stored in eCB and used primarily as a point of contact to notify schools of actions taken specify to them and to make inquiries regarding the campus-based programs.

(2) Contact information for state agencies will be posted with the Teacher Cancellation Low Income (TCLI) Directory and will be available to the public for information on schools that qualify as low income.

(3) Contact information for Perkins Loan recipients that are delinquent in repaying their loans will permit FSA to mail a letter to the borrowers encouraging them to contact their schools and enter into new repayment agreements.

(4) Financial information will be used to calculate the amount of funding to be made available for the schools participating in the campus-based programs and to account for the funding levels they have been awarded in previous years.

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

No, this information will not be 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.**

There will be a compliant posted Privacy Notice.

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.

Physical and environmental protection will be provided by the Virtual Data Center (VDC). Briefly, these controls consist of physical access control, contingency planning/disaster recovery, data backup, uninterruptible power supply, fire and natural disaster protection, network and communications protection (including firewalls, intrusion detection, antivirus protection, and encryption), hardware maintenance, and logical access control. See sections 3 and 4 of the VDC System Security Plan for a detailed explanation. All users must also undergo annual security awareness training, and some personnel are required to take specialized training as well.

In addition, the following logical access controls are also provided.

(1) Authentication Control. To access the eCB system, users must be authorized by the Destination Point Administrator (DPA) and have a PIN and a Title IV Gateway (TG) number. ED Administrative Users (Admin Users) have the additional option of accessing the eCB system through use of an ID (see below for requirements and procedures).

School users are allowed to access data only from the schools associated with that specific TG number.

(2) School Users/Servicers. The school user or servicer must be logged onto the Internet and have a Web browser open. The PIN serves as the user's identifier, allowing the user to access information in systems for the Department of Education. To obtain a PIN, users must go to www.pin.ed.gov to apply.

The PIN contains four characters and is combined with information about the user (the first two letters of the last name, the date of birth, and the Social Security Number) to create a unique PIN number. These items help assure individual accountability on the system.

The required TG number must be associated with the award year the user is trying to access. To obtain a TG number, or to get an existing TG number associated with the current award year, users must visit the Student Aid Internet Gateway (SAIG) Web site: www.fsawebenroll.ed.gov. The TG number contains five characters and is associated with a particular school. A school that already has a TG number can contact its DPA to obtain access to the desired award year(s).

(3) Alternative Identification and Authentication for ED Users. Authorized Education users have the option of authenticating directly with the eCB application without going through the PIN Web site authentication process. This functionality is named the Admin Login by ID module. Only the eCB System Security Officer (or his or her designees) can grant Admin Login by ID access to other Education and contract users.

a. Admin Login by ID requirements:

- Only the Security Officer can authorize and generate login IDs.
- Passwords must be between 8 and 16 characters.
- Passwords must contain at least two alphabetic characters.
- Passwords must contain at least one number or special character.
- Passwords cannot match any of the last three passwords used.
- Passwords expire after 90 days.
- Passwords will only be reset after the Security Officer verifies the mother’s maiden name password reset.
- Users cannot change their passwords more than once a day.
- Users are forced to change their passwords after reset.

The basic flow of events for Identification and Authentication follows:

b. Access Procedures Using the PIN

- The user enters the eCB URL into the browser address window.
- The system displays the eCB welcome page. The first part of the page contains a welcome message and general login information. At the center of the page is a Login button. Below this link are instructions for the user on how to get a PIN, how to get a TG number, and what to do if the school is new to the eCB programs. There is also a privacy policy and a 508 compliance statement.
- The user selects the Login button. Users who have their browsers set to display a security warning might see a security message.
- The system sends the user to the PIN Authentication site, which is outside of the eCB system.
- The user enters his or her Social Security number, first two letters of the last name, date of birth, and the PIN, and then selects the Submit Request button to continue authentication. The PIN site sends the user back to the eCB system after successful authentication. If authentication is unsuccessful, users are requested to reenter the information.
- The system displays a screen where the user enters a TG number for the FISAP to be accessed. There is a field to enter the number.
- When the user enters the TG number and selects “Next,” the user’s data string is sent to Title IV WAN for assigning access rights.
- The System displays the appropriate page for the designated user type—School user or Servicer.
- The user can now work on the FISAP.

c. Access Procedures Using Admin Login by ID

- The user enters the eCB Administrative-Side URL into the browser address window.
- The system displays the eCB Education-Side welcome page.
- The user selects the Login Using Login User ID/Password.
- The system sends the user to the Login using the user ID page.
- The user enters the assigned Login user ID and password.
- Upon successful authentication, the user is redirected to the eCB Administrative-Side front page.
- No digital or electronic signatures have been approved for use at this time. There are no policies for bypassing user authentication.
- There are a limited number of access attempts permitted. For Admin Login by ID, access is cut off after three attempts.
- All personnel granted access to the eCB system are cleared through a security screening process. The system verifies users by cross-indexing various data fields, as explained above. This information is verified against the information input into the SAIG system to make sure the user is actually the person given access to the TG number.

(4) Password Controls. There are no passwords involved for access to the FISAP using the PIN. See the preceding section for passwords associated with the Admin Login by ID function.

(5) Access Privileges. Controls are in place to authorize or restrict the activities of users and personnel within the application/system. Hardware and software features are designed to permit only authorized access to, or within, the application/system, restricting users to authorized transactions and functions.

User interface services are physically or logically separated from information storage and management services. Information is stored on servers at the VDC, and users have different computers.

As mentioned earlier, to log into the eCB Web site, users must have a valid PIN and TG Number (unless they are logging into the Administrative side of the eCB Web site using Admin Login by ID). Users can apply for an FSA PIN by logging onto www.pin.ed.gov.

The eCB SSO maintains a manual access control list of users that details the access rights. The eCB Administrative-side Web site security module lists users and the modules they have access to. In addition, periodic reviews are done to remove users that no longer require access to eCB.

System developers must have an access request form signed by the eCB SSO. The SSO must then request the VDC to set up access to the HP eCB directory and to the HP Oracle eCB database. To access the Administrative side of the eCB Web site, an access request form must be submitted to the SSO, who will set up access through the SAIG enrollment form and the eCB administration security module to allow access to certain modules within the site. The separation of duties between the SSO and the VDC prevents any single individual from having all necessary authority or information access. User access is limited by the type of access the SSO allows.

(6) Session Controls. The application/system automatically locks users out of the system after a 30-minute period of inactivity on the School side and a 60-minute period of inactivity on the Administrative side. Each person who signs on to the eCB system gets a separate session; that is, the timeout feature applies only to that individual's session, not to someone else's. However, users are allowed multiple logon sessions; there are no limits to the length of the sessions.

(7) Re-Certification of Users. The System Security Officer (SSO) will annually send a new SAIG User Statement (used as the eCB Rules of Behavior) to each eCB user. The user must fill out and sign the form and return it to the SSO by the SSO's deadline. If the user fails to return the SAIG User Statement, the SSO will delete the user's access and make note on the user's User Access Request Form on file that the user failed to re-submit the SAIG User Statement.

Periodically, the SSO will check the age of the User Access Request Forms on file. If the dates are aged, the SSO will contact the user to submit a new, up-to-date form.

(8) Encryption. To ensure data integrity, the eCB Web Application uses the SHA-1 encryption algorithm to store sensitive plaintext information that will be used later to for one-way comparison against the initially ciphered plaintext information. For system-to-system and/or system-to-client communication, the self-protection techniques for the user authentication mechanism include 128 bit Secure Socket Layers 2.0 between the eCB Web site and the client and Cert-J Encryption for information traveling between the eCB Web site and the Title IV Mainframe.

(9) Audit Trails. User accountability is tracked through the PIN Web site and through unique user IDs with eCB. The eCB system monitors users to verify user identities and to ensure personal accountability. If you try to log on with three unsuccessful attempts, you will be locked out of the system and will have to have your user ID or pin reset.

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

Yes, a system of records is being created with the collection of this information.

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

http://www.cbfisap.ed.gov/
http://www.tcli.ed.gov/ (will be active in September 2005)
http://www.cbfisap.ed.gov/CBSWebApp/admin/adminWelcome.jsp