Privacy Impact Assessment for the

Student Aid Internet Gateway (SAIG)

Date
May 1, 2008

Contact Point
System Owner: Phillip Wynn
Author: Reza Venegas (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
   Last Four Digits of SSN (required)
   Phone
   Email

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

   (1) The information is only being collected to create administrative accounts to access the Transaction Delivery Community Manager.

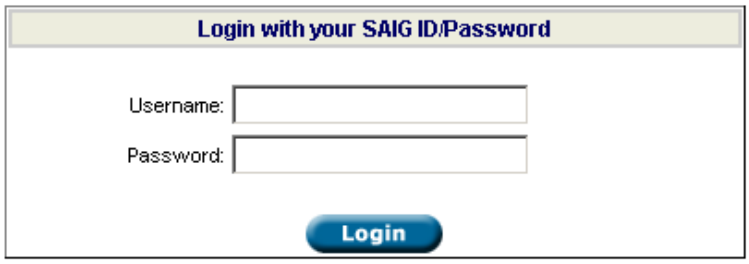
3. **How will FSA use this information?**

   This information is stored in a database for historical records only.

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.**



This is a U.S Government system, to be used by authorized personnel only. If you use this computer system, you should understand that all activities may be monitored and recorded by automated processes and/or by Government personnel. Anyone using this system expressly consents to such monitoring.

WARNING:

If such monitoring reveals possible evidence of criminal activity, monitoring records may be provided to law enforcement officials. This system contains personal information protected by the Privacy Act of 1974 (as amended). If you use this computer system, you are explicitly consenting to be bound by the Acts requirements and acknowledge the possible criminal and civil penalties for violation of the Act.

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.

SAIG reviews: account management processes, account establishment, activation, modification, disabling, and removal. SAIG also reviews periodically for account reviews and disablement. AppDetective and Nessus are used to test account management.

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.

At the system level a report is run for current users quarterly. Vangent sends the SAIG SSO a list of current users to verify current status. The permissions that are granted have to be approved by the government SSO and supervisors. The VDC contractor (VDC Contractor) works on the operating system/hardware level.

Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by SAIG to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. 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?

The information collected to create accounts is stored in a database, in the application environment. All other information that passes through the system is encrypted and therefore can not be ready by SAIG.

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

https://www.saigportal.ed.gov/saigprod/portal.jsp
http://www.ed.gov/notices/pia/cod.pdf