Privacy Impact Assessment
For
SAIG Participation Management (PM)

Date:
MAY 27, 2010

Point of contact:
Calvin Whitaker
202-377-3045
Calvin.Whitaker@ed.gov

System Owner:
Keith Wilson
202-377-3591
Keith.Wilson@ed.gov

Author:
Calvin Whitaker
202-377-3045
Calvin.Whitaker@ed.gov

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.

The Federal Student Aid (FSA) Student Aid Internet Gateway (SAIG) Participation Management (PM) system allows organizations to enroll for electronic access to Federal Student Aid systems. All users who require access to Federal Student Aid systems must provide the appropriate authorization. The purpose of SAIG PM is to provide eligible organizations an enrollment process to participate in exchanging Title IV program data. Organization's are required to assign a Primary Destination Point Administrator (Primary DPA) to enroll for the services in which they are approved to participate, as well as assign authorization levels and general access to Federal Aid Systems through SAIG PM to other members of the Primary DPA's campus or organization.

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?

Title IV of the Higher Education Act of 1965, as amended (HEA); 20 U.S.C. 1070 *et seq.* The collection of Social Security numbers of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008)

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?

The elements of PII data collected and maintained by the system include:

Social Security number (SSN), names (first and last), date of birth (DOB), telephone number, address, and mother's maiden name.

The sources of the information include student financial aid administrators and authorized employees or representatives of: postsecondary institutions, third party servicers, lenders, guaranty agencies, state scholarship programs, states agencies, and local educational agencies, and schools offering secondary level of instruction.

The information is collected primarily via a Web-based enrollment process; however there is a paper enrollment process as well.

Yes. SAIG Enrollment cross-references multiple databases for the authenticating users who are eligible to participate in the electronic exchange of data with the Department of Education systems listed below. The types of data exchanges are the transmission of files to and from the following Department of Education databases and the user access to these system's websites on line.

- Common Origination and Disbursement (COD) System (common record batch transmission only)
- Central Processing System (CPS)
- Electronic Campus-Based (eCB) System

- National Student Loan Data System (NSLDS) (on line)
- Financial Management System (FMS)
- Debt Management Collection System (DMCS)
- Title IV Additional Servicers (TIVAS)
- Access Information Management System (AIMS)
- Common Services for Borrowers (CSB)
- Direct Loan Servicing System (DLSS)
- Postsecondary Educational Participants System (PEPS)

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 (internally and externally) identified and how they were mitigated.

The information is necessary to the mission of the Agency in order to comply with the HEA policies, regulations and statues.

The privacy risks identified include the loss of data, stolen data, identity theft and misuse of data. These risks have been mitigated though, access authentication and, security and intrusion detection software. All security vulnerabilities that are identified are tracked and migrated through the Operational Vulnerability Management System (OVMS).

5. **Social Security Numbers - If an 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. **If system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent. If no SSN is collected, no signature is required.**

Yes, SSN's are collected to determine if any users or potential users are in default on an obligation to the U.S. Department of Education. NSLDS stores (as stated in the NSLDS system of records notice (SORN)) user PII and runs a monthly sweep of all users – anyone who subsequently enters into default will lose their access rights and the Department will disable the defaulted user's access to all Departmental systems.

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.

Internal uses of the information include the sharing of enrollment information between FSA systems including the National Student Loan Database System (NSLDS), Financial Management System Lender Reporting System (FMS/LaRS) , Direct Loan Servicing System (DLSS), Authentication Identification Management System (AIMS) and, Common Origination Disbursement (COD), Title IV Additional Servicers (TIVAS), Debt Management Collection System (DMCS), Electronic Campus-Based (eCB) System, Common Services for Borrowers (CSB), Postsecondary Educational Participants System (PEPS) and the Central Processing System (CPS)

The information is used externally. The external entities include:

- Freedom of Information Act (FOIA) Advice Disclosure
- Contracting Disclosure
- Litigation and Alternative Dispute Resolution Disclosure
- Research Disclosure
- Congressional Member Disclosure
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Employment, Benefit, and Contracting Disclosure
- Employee Grievance, Complaint or Conduct Disclosure
- Labor Organization Disclosure

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?

The purpose of the information shared is to provide user authentication to obtain access to FSA systems.

The Department may disclose information in this system without the consent of the individual, in accordance with the provisions of the Privacy Act of 1974.

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 with another agency?

Yes, the Department may disclose information in this system without the consent of the individual, in accordance with the provisions of the Privacy Act of 1974, Privacy Protection Act of 1989 and OMB Circular A-130. The information shared includes but is not limited to: SSN, DOB, legal addresses, first and last names, and e-mail addresses.

The external entities for disclosure include:

- Program Disclosure
- The Department may disclose records maintained in the SAIG, Participation Management System for the purpose of allowing authorized users who are eligible to participate in the electronic exchange of data with the Department to transmit files to and from the following
- Department databases and access the Department's websites on line, based on the approved program functions of each of the Department's systems that include, but are not limited to the following:
- (a) COD System;
- (b) CPS, under the Federal Student Aid Application File;
- (c) eCB System;

- (d) NSLDS;
- (e) FMS;
- (f) DMCS, under Common Services for Borrowers (CSB)
- (g) TIVAS;
- (h) AIMS and;
- (i) DLSS;
- Freedom of Information Act (FOIA) Advice Disclosure
- Contracting Disclosure
- Litigation and Alternative Dispute Resolution Disclosure
- Research Disclosure
- Congressional Member Disclosure
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Employment, Benefit, and Contracting Disclosure
- Employee Grievance, Complaint or Conduct Disclosure
- Labor Organization Disclosure

These disclosures may be made on a case by case basis or, if the Department has complied with the computer matching requirements of the Privacy Act, under a Computer Matching Agreement (CMA) that is authorized and approved prior to the sharing of data.

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?

A notice is provided to the user prior to the collection of his or her information. The Privacy Act provides the individual the ability to access his or her account and the right to request an amendment of any inaccurate information in his or her record. The individual may request the information in his or her record from ED by calling 1-800-330-5947 or via e-mail by sending an e-mail to: CPSSAIG2ed.gov. A full explanation of the individual's rights under the Privacy Act is set forth in the Department's Privacy regulations Part 5b.

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

http://www.fsawebenroll.ed.gov

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 security safeguards in place include but not limited to:

- Audit Trails
- Signed Rules of Behavior

- OMB Clearances
- Security Awareness Training
- Vulnerability scanning
- Change Management Process
- Separation of Duties
- Continuous Monitoring
- Annual Auditing
- System Authentication for access
- System Firewalls
- Intrusion Detection Software
- System Required User Ids and Passwords

The CPS SAIG PM last Security Authorization (SA) was granted on July 25, 2008 and is compliant with all Federal Security requirements (OMB Circular A-130, NIST 800-53 and FISMA).

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?

This system is covered under the system of records notice entitled "Student Aid Internet Gateway (SAIG), Participant Management System, April 19, 2010 (75 FR 20346)).

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:

Yes, the SAIG PMS has records retention and disposition schedule numbers from NARA.

These records are covered by the General Records Schedule (GRS) 24, Item 6(a). The retention requirement is to destroy/delete the record 6 years after the user account is terminated or password is altered or when no longer needed for investigative or security purposes whichever is later.

NARA Job No. NC-12-75-1 and NARA Job No. NC 12-80-2 and GRS 20.