Privacy Impact Assessment
For
FFELP Student Loan Servicing System

Date:
September 29, 2010

Point of contact:
Mark Dunning, 310-847-5347, mark.dunning@acs-inc.com
Bryan Robinson, 310-847-5343, bryan.r.robinson@acs-inc.com

System Owner:
ACS Education Services

Author:
Bryan Robinson, 310-847-5343, bryan.r.robinson@acs-inc.com

Office of
Federal Student Aid

U.S. Department of Education (DoED)

Expiration Date:

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 Financial Education Loans Program (FFELP) is the student loan servicing program that is developed in-house and its primary functions are origination, maintenance, billing, and collections of FFELP and private student education loans. The departments that use the FFELP system are Client Accounting, Client Relations and Marketing, Clients and Guarantors, Collections/Skip-Trace, Conversions/Sales, Customer Service, Default Service, Internal Audit, Lender Service, Mail Service, Monetary Processing, Research Group, and Transaction Processing. These departments are housed throughout the various ACS Education Service's SBUs in Long Beach, CA; Utica, NY; Aberdeen, SD; Canyon, TX; and Madison, MS.

The servers that house the software for FFELP are based in Dallas, TX, within the ACS data center. They are composed of three HP ES40 Alpha (OpenVMS) servers, two IBM RS/6000 (AIX/Oracle), 87 Wintel 2000/2003 (all the Wintel servers are in the process of upgrading to 2003) servers, and one Sun Sunfire V240.

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?

Federal Information Security Management Act of 2002 (FISMA)
Information Technology Management Reform Act of 1996, (Clinger-Cohen Act) 44 U.S.C. 3501
Computer Fraud and Abuse Act of 1986, 17 U.S.C. 1201
Homeland Security Presidential Directive 7
Presidential Decision Directive 67 (PDD 67)
Privacy Act 1974, 5 U.S.C. 552a
Trade Secrets Act
OMB Circular A-130, Management of Federal Information Resources
Federal Records Act of 1950, as amended, 44 U.S.C. 2901
Authority: Executive Branch Directives
Paperwork Reduction Act, 44 U.S.C. Chapters 29 and 35
Freedom of Information Act (FOIA), as amended, 5 U.S.C 552
Computer Security Act of 1987, 44 U.S.C. 3504
Gramm Leach and Bliley of 1999, 15 U.S.C. 6801-6809

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?

In order for borrower (student) to create a personal account within FFELP he/she must provide their name, SSN, date of birth, zip code, and email address. This is information is provided by the individual borrower via email, using ACS web survey forms, or through the mail in hardcopy format.

ACS Education Services does link this information in the RDB (Oracle) databases within the FFELP system for tracking, retention, and analytical purposes.

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 identified and how they were mitigated.

Personal information provided by the borrower is collected so ACS Education Services can address any issues specific to that individual borrower's situation. Information collected from the website will be used to help determine the effectiveness of the website as a customer service tool and improving the services of ACS. Information collected on the online forms will be used in order to process that form to begin servicing the loan.

ACS Education Services is aware of the risks associated with collecting personal information via e-mail and thru online applications. Information submitted online will be collected by the cookies attached the browser. When a borrower is accessed within the website, their information will be stored on the cookies during the duration the user is on the site. Once the user has logged-off the website, the cookies will and information about the borrower's user session will be automatically destroyed so it will not be permanently stored on the borrower's computer. Personal information that is submitted by email is protected by 128 bit encrypted secure socket layer that uses public key cryptography (which also secures the website).

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.

The social security number must be provided when completing the forms online per compliance to the Higher Education Act of 1965 sections 483 (20 U.S.C. 1090) and 484 (20 U.S.C 1091). In order to obtain a user account, borrowers must submit their SSN, date of birth, name, zip code, and email address. Borrowers have the option of typing in their SSN at any time during the user registration process. The submission of the social security number from the borrower is under these disclosures:

- Freedom of Information Act (FOIA) Advice Disclosure
- Disclosure of the Department of Justice
- Contract Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosures
- Research Disclosure
- Congressional Member Disclosure
- Disclosure for Use by Law Enforcement Agencies
- Enforcement Disclosure
- Employment, Benefit, and Contracting Disclosure
- Employee Grievance, Compliant or Conduct Disclosure
- Labor Organization Disclosure
- Disclosure to Providers of Web-based Postsecondary Education Admission Applications

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.

ACS Education Services uses this information to verify the existence of loans. This information will be used by the Department of Education and ACS for these services:

- Provide information targeted to the user, based on requirements and criteria provided by the user (information about the loans)
- Store the search results for later retrieval
- Assist ACS Education Services to target financial aid and college information to specific audiences based on demographics provided by the users. The demographic data will not be linked to the personal information to identify individuals. The demographic dated will be used to determine populations of website users that would benefit from specific programs, opportunities, and updates.
- Respond to request sent via e-mail.
- Analyze the overall satisfaction with the website and its various features, assess the website's success, and determine how to enhance the site itself and its features.

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? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

The borrowers' personal information is shared for collection purposes with the Federal Student Aid (FSA). The FSA must have a Memorandum of Understanding (MOU) and a Trading Partners Agreement (TPA), per compliance to OMB Circular A-130, Appendix III, with ACS in order to have this information shared. The MOU documents the business and legal requirements necessary to support the business relations among the organizations. In addition to an MOU, a trading partner must also have an Interconnection Security Agreement (ISA). The ISA is used to establish the requirements for the data exchange between the organizations. The TPA establishes the management agreement between the business lines regarding development, management, operation, and security of a connection between internal entities. The FSA must show that its control environment meets all the requirements documented on the ISA and TPA in regards to securing the PI.

However, FFELP does not employ system interconnections because all sharing of information is through ADE (ACS Data Exchange - FTP) indirectly and this does not constitute interconnecting systems as defined by NIST.

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 wit another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The personal information provided by the borrowers will be shared with the Department of Treasury and the Internal Revenue Service (IRS) under the disclosures listed for question 5. These disclosures may be made on a case-by-case basis. ACS ES will only share information with an external organization only if it has a Memorandum of Understanding (MOU) and Trading Partners Agreement (TPA) under OMB Circular A-130, Appendix III. There will be no sharing of information outside the purpose of collecting information and being compliant to the MOUs and TPAs. The MOU documents the business and legal requirements necessary to support the business relations among the organizations. In addition to an MOU, a trading partner must also have an Interconnection Security Agreement (ISA). The ISA is used to establish the requirements for the data exchange between the organizations. The TPA establishes the management agreement between the business

lines regarding development, management, operation, and security of a connection between internal entities. Below are the organizations that have MOUs and TPAs with ACS.

However, FFELP does not employ system interconnections because all sharing of information is through ADE (ACS Data Exchange - FTP) indirectly and this does not constitute interconnecting systems as defined by NIST.

FFELP Trading Partners:

ACS Education Solutions
Credit Bureaus
Guarantor Agencies
Lenders
BNY Mellon
NCP Solutions
National Student Loan Data System (NSLDS)
Schools

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?

The site displays the following to the borrowers when they access it:

"We collect no personal information about you unless you choose to provide the information to us. When we do collect information about you, we only collect information that we need to provide you or someone in your family student financial assistance."

The borrowers are also notified that providing their information on the website will constitute consent to all uses of their information for the site and there is no option given that affirmatively consents of certain uses of their information.

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

www.ed-servicing.com is the website that has the Privacy Notice displayed within it.

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?

Personal information of the borrowers is protected physically, technically, and administratively. The servers that house the FFELP system are located within the data center in Dallas, TX, which is secured by badge readers, third party security, CCTV cameras, and alarms throughout the facility. When the personal information is backed up and stored within magnetic tape, those tapes are encrypted to ensure confidentially and protection when stored off-site. In addition, the access badge listings are reviewed every quarter to ensure that all the personnel that have access to the servers are appropriate. The data files are logically secured by restrictive access through authentication of the Windows AD network and the OpenVMS operating system, access control

listings that are monitored every quarter by the HelpDesk, and built-in password parameters within Windows AD and the OpenVMS operating system. User access is also monitored by tracking user activity within the system logs which are reviewed daily by the FFELP administrator. User access is re-validated every quarter to ensure the appropriate access to the data files is given to the proper personnel. Access and the type of access to these files are not given without proper manager's approval which is documented and retained. Furthermore, when an employee is terminated their users access is deleted within 24 hours after termination both logically and physically. The network and the website is protected by a 128bit encrypted SSL. To see more detail of the controls within the control environment, please see the System Security Plan (SSP).

In addition, Certification and Accreditation for FFELP is conducted in accordance with the DOE Handbook for Information Technology Security Certification and Accreditation Procedures and FSA policies and procedures by an independent certification team, the Certification Review Group (CRG). FFELP undergoes reviews by the CRG at least every three years or when a major program has been added to the system. The last certification and accreditation review was performed in September 2008.

These controls are compliant to the regulations and standards listed below:
-Federal Information Control Audit Manual (FISCAM)
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems, Nov. 2001
- NIST SP 800-30 Risk Management Planning Guide for Information Technology Systems, Jan. 2002
- NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-35 Guide to Information Technology Security Services, Oct. 2003
- NIST SP 800-37 Information Technology and Accreditation Guide, Oct. 2003
- NIST SP 800-40 Procedures for Handling Security Patches, Aug. 2002
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy, Jan. 2002
- NIST SP 800-42 Guidelines on Network Security Testing, Oct. 2003
- NIST SP 800-44 Guidelines on Security Public Web Servers, Sept. 2002
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems, Sept. 2002
- NIST SP 800-50 Building an Information Technology Security Awareness Program, second draft, Apr. 2003
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems, July 2003
- NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- NIST SP 800-60 Volume 2, Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- NIST SP 800-64 Security Considerations in the Information Systems Development Lifecycle, Oct. 2003
- NIST Special Publications 800-53, Rev. 3, Aug. 2009, Recommended Security Controls for Federal Information Security Systems.

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?

A system of records has been created under the Privacy Act, 5 U.S.C. 552a. Borrowers are provided notice of their rights under the Privacy Act via links to the agency Privacy Act regulations (5 C.F.R. Part 5b) and to the Privacy Act system of records notice for the website.

In addition, the FFELP system is compliant to the SORN 2010-8959, Apr. 16, 2010, as being a covered application under the SAIG system.

13. **<u>Records Retention and Disposition</u>. 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:

ACS Education Services does have a records retention and disposition policy and schedule which are compliant to the applicable federal, state, and international legal requirements and any contractual obligations as stated in the contract by the client.

Certifying Officials Signatures:

_____	_____
System Owner	**Date**
_____	_____
Program Office Computer Security Officer	**Date**

For systems that collect, maintain and or transfer SSNs:

_____	_____
Senior Program Official	**Date**