Privacy Impact Assessment

For:
ACS Education Servicing System (ACES)

Date:
10/24/2012

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

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

Author:
Brian Sowl
303-696-5278
Brian.Sowl@Nelnet.net

Federal Student Aid

U.S. Department of Education

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 ACS Education Servicing System (ACES) environment is used by clients to service Federal Student Aid (FSA) Title IV Student Loan Processing environment. Operational capabilities of the system include borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, collection, skip-tracing, claims and correspondence history files. ACES communicates with the internal FSA platforms, borrowers, educational institutions, lending institutions, other loan servicers, third-party data providers, consumer reporting agencies, guarantors and government agencies (as permitted by the Federal Privacy Act of 1974). Channels of communication include mail, phone calls, a secure borrower website, email and secure data transfer links.

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?**

   The Higher Education Act of 1965 (HEA), As Amended, Section 441 and 461 Title IV, Section 401.

3. **Characterization of the Information. What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? 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 following elements of Personal Identifiable Information (PII) are received from the prior servicer at the time the loan is converted to ACES for servicing of government owned loans. Information is maintained through changes requested by the borrower via written correspondence, borrower call or borrower electronic request using Manage My Account.

   The ACES system retrieves, stores, and presents the following elements of PII:

   - Full Name
   - Maiden Name
   - Social Security Number (SSN)
   - Driver's License Number and State
   - Home Address
   - Home, Work, Alternate and Mobile Telephone Numbers
   - Email Address
   - Employment Information
   - Financial Information
   - Medical Information (to the extent required for purposes of certain deferments and discharge requests)
   - Bank Account Numbers
   - Related Demographic Data
   - Borrower Loan Information, including: disbursement amount, principal balance, accrued interest, loan status, repayment plan, repayment amount, forbearance status, deferment status, separation date, grace period and delinquency
   - Alien Registration Number
   - Student Loan Account Numbers.

Sources of PII include borrowers, co-borrowers, educational institutions, the U.S. Department of Education(DoED), National Student Loan Data System (NSLDS), National Student Clearinghouse, and other authorized and/or reliable third parties including but not limited to FSA contractors, borrower references, U.S. military, commercial person locator services, national consumer reporting agencies, financial institutions, and U.S. Department of Treasury.

Information is collected via paper, website, on-line, electronic data transmission, and telephone.

The information is used to link or cross-reference multiple internal ACES databases. Refer to Question 1 hereof.

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 any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The PII is necessary to properly service Federal student loans according to the regulatory requirements of Title IV Servicing. The SSN is never included in any electronic or postal mailings.

The borrower name, address, email address, and phone numbers are essential for communicating with the borrower and performing collection activities. The endorser's name, address, and phone numbers are used to reach the borrower when conventional methods fail.

The risk is that PII may be obtained by an unauthorized party to commit fraud and identify theft. The following are mitigation steps in place.

- Associates with the ability to access this information require a personnel security clearance before access is granted
- System access is assigned based on job function requirements and are maintained through access controls
- The change management process includes separation of duties
- Associates are required to complete Security Awareness Training annually
- Physical access to areas where PII data is available is secured with a security badge system to limit physical access to areas as required
- Annual risk assessments are performed.

5. Social Security Number (SSN). 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 designee. If no SSN is collected, no signature is required.

The SSN is the unique identifier for Title IV programs and its use is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. Trading partners include the Department of Education, Internal Revenue Service, Department of Homeland Security, Selective Service System, institutions of higher education, national credit bureaus, lenders, and servicers.

Borrowers (and endorsers, if applicable) are advised of the collection and use of the SSN in the promissory note materials of their Title IV program loans. In accordance with state laws regarding the use of SSN's, a proprietary account number is assigned by ACES and utilized for all borrower and

endorser communications in lieu of the SSN except where a SSN is required on a federal form. The proprietary account number is also used for the purposes of internal reporting and communications.

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.**

   This information is collected to meet the contractual requirements of Federal Student Aid, enabling ACES to perform student loan servicing activities.

   The information is used for identification and verification purposes. Information is also used to assist borrowers with managing their loans, determine borrower eligibility for entitlements such as deferments, forbearances, and discharges, and to locate borrowers in cases of invalid addresses and/or phone numbers.

   External uses of the information include reporting to schools for purposes of default management and program eligibility, consumer reporting agencies for the purposes of reporting and maintaining borrower credit history.

   The data is analyzed/evaluated by ACES for purposes of maintaining account balances, debt collection, default prevention, applying deferments and forbearances, and general account maintenance.

   Sources of information will be various Federal agency databases, servicers from whom the Department of Education purchases student loans, person locator services and consumer reporting agencies.

7. **Internal Sharing and Disclosure**. **With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?**

   ACES shares this information with:

   - Federal Student Aid and its agents and Contractors
   - National Student Loan Data System (NSLDS)
   - Debt Management Collection System (DMCS)
   - Common Origination and Disbursement System (COD)
   - Student Aid Internet Gateway (SAIG)
   - Total AND Permanent Disability (TPD).

   All or part of the information described in Question 3 hereof may be shared.

   The information is only shared as required by Federal Student Aid.

   See response to Question 4 hereof for risks and mitigation measures.

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 or other type of approved sharing agreement with another agency?

The ACES system does not share PII or other information with any external entities, except to process and service federal student loans and as permitted by the Privacy Act of 1974 and as required by Federal Student Aid.

Information will be shared with the following non-Department of Education systems and governmental entities:

- Internal Revenue Service, (including Adjusted Gross Income requests, waiver image processing and 1098/1099)
- U.S. Department of Treasury ("Treasury") (including Lockbox, Electronic Development Application vendor, Pay.gov, Remittance Express, Integrated Professional Automation Computer, and Ca$hLinkII)
- United States Postal Service.

Information will be shared with the following nongovernmental entities:

- Educational Institutions
- Other Federal Loan Servicers
- Independent Auditors
- National Consumer Reporting Agencies
- Person Locator Services
- Other parties as authorized by the borrower.

All or part of the information described in Question 3 hereof may be shared.

The information is only shared as required by Federal Student Aid.

Information is shared through file transmissions and secure email transmission using encryption methods compliant with Federal requirements.

Sharing of information with nongovernmental entities (consumer reporting agencies, independent program participants, etc.) will be pursuant to contractual or regulatory requirements, or through sharing agreements between the applicable entities and the Department of Education.
See response to Question 4 hereof for risks and mitigation measures.

9. **Notice. I**s **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 privacy notice/policy is presented to the borrower via the following channels:

- Pursuant to the Gramm-Leach-Bliley Act, DoED's privacy notice is sent to the borrower by letter or email upon purchase of the loan by DoED and on an annual basis thereafter for the life of the loan

- A privacy notice is provided on the Free Application for Federal Student Aid (FAFSA) form and on the FAFSA online application website (www.fafsa.ed.gov)
- A privacy policy is also posted on ACES secure borrower portal websites (http://www.nelent.com; http://myfedloan.org, https://accountaccess.myfedloan.org)
- In order to establish an online account on the ACES system secure borrower portal website, the borrower must agree to the Term of Service which incorporates the privacy policy by reference and link.

Borrowers can at this point decline to provide additional information: however, providing certain information is required in order to communicate with ACES through its secure borrower website and/or customer service call center.

Borrowers are required to opt into online account access features, and are required to provide consent, in compliance with applicable law, for various features and services provided by the ACES system, such as paperless document delivery and online payment services.

ACES shares information with designated financial, education, and Department of Education organizations and contractors only as required by contract.

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

http://www.nelnet.com
http://www.myfedloan.org
https://accountaccess.myfedloan.org.

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 C&A been completed? Is the system compliant with any federal security requirements?

Physical access to areas where PII data is available is secured with a security badge system to limit physical access to areas as required.

ACES also employs the following technical safeguards:

- Firewalls and existing proxy servers are in place to control external access to internal resources
- Connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the Nelnet boundary
- ACES physically allocate publicly accessible information system components (e.g., public web servers) to separate sub-networks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated
- All routers, switches and firewall are configured to allow only specifically authorized services and traffic (Deny-By-Default)
- All DoED data access is available to authorized and approved users with a 5C or 6C security clearance
- Privileged access to ACES is limited to only 6C security cleared personnel
- Signed Rules of Behavior and Security Awareness training for all employees

- Two Factor Authentication is not yet implemented on ACES yet. It will be implemented on this system later this year
- In accordance with the Federal Information Security Management Act (FISMA), ACES received an Authority to Operate (ATO) from FSA on December 12, 2011.

The ACES system is compliant with the following Federal Standards and Guidelines:

- Federal Information Security Management Act (FISMA)
- Privacy Act of 1974
- E-Government Act of 2002
- Federal Information Security Controls Audit Manual (FSICAM)
- Federal Information Processing Standards Publications (FIBS PUBS) on IT Security
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
- NIST SP 800-35, Guide to Information Technology Security Services, October 2003
- NIST SP 800-37, Rev. 3, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- NIST SP 800-40, Procedures for Handling Security Patches, November 2005
- NIST SP 800-41, Guidelines on Firewalls and Firewalls Policy, September 2009
- NIST SP 800-42, Guidelines on Network Security Testing, October 2003
- NIST SP 800-44, Rev. 2, Guidelines on Security Public Web Servers, September 2007
- NIST SP 800- 45, Rev. 2, Guidelines on Electronic MAIL Security, February 2007
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002
- NIST SP 800-50, Building an Information Technology Security Awareness Program, October 2003
- NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-55, Rev. 1, Performance Measurements Guide for Information Security, July 2008
- NIST SP 800-58, Security Considerations for Voice Over IP System, JANUARY 2005
- NIST SP 800-60, Rev. 1, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-61, Rev. 1, Computer Security Incident Handling Guide, March 2008
- NIST SP 800-64, Rev. 2, Security Considerations in the Systems Development Life Cycle, October 2008
- NIST SP 800-65, Integrated IT Security into the Capital Planning and Investment Control Process, January 2005
- NIST SP 800-70, Rev. 2, National Checklist Program fir IT Products: Guidelines for Checklists Users and Developers, February 2011
- NIST SP 800-77, Guide to IPsec VPNs, December 2005
- NIST SP 800-81, Rev. 1, Secure Domain Name System (DNS) Deployment Guide, April 2010
- NIST SP 800-83, Guide to Malware Incident Prevention and HANDLING, November 2005
- NIST SP 800-88, Guidelines for MEDIA Sanitization, September 2006
- NIST SP 800-92, Guide to Computer Security Log Management, September 2006

- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- NIST SP 800-95, Guide to Secure Web Services, August 2007
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
- NIST SP 800-113, Guide to SSL VPNs, July 2008
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, April 2010
- NIST SP 800-123, Guide to General Server Security, July 2008
- NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008.

Department of Education Policies:

- Department of Education Handbook for Information Technology Security
- Department of Education Handbook for Information Technology Security General Support System and Major Application Inventory Procedu**res**
- Department of Education Handbook for Certification and Accreditation Procedures
- Department of Education Handbook for Information Technology Security Configuration Management Procedures
- Department of Education Handbook for Information Technology Security Contingency Planning Procedures
- Department of Education Information Technology Security Test and Evaluation Plan Guide
- Department of Education Incident Handling Program Overview
- Department of Education Handbook for Information Technology Security Incident Handling Procedures
- Department of Education Information Technology Security Training and Awareness Program Plan.

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?

ACES is covered under the "Common Services for Borrowers" System of Record Notice (SORN), which was published as number 18-11-16 in the *Federal Register* on January 23, 2006 (71 FR 3503-3507).

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:

Per FSA, ACES will follow the "FSA Loan Servicing, Consolidation, and Collections Records" records schedule. The ACS Tracking Number is OM: 6-106:l74.

DoED Record Schedule:
Schedule Locator NO: 075
Draft Date: 03/11/2009
Title: FSA Loan Servicing, Consolidation and Collections Records

Principal Office: Federal Student Aid

NARA Disposition Authority: N1-441-09-16

Description:

These records document business operations that support the servicing, consolidation, and collection of Title IV federal student aid obligations. These records relate to the post-enrollment period of student aid, including servicing of direct loans, consolidations of direct loans, managing and recovering defaulted debts assigned to the Department from Federal Family Educational Loan (FFEL) and other lenders, rehabilitated loans, and any other type of Title IV student aid obligations.

This schedule provides a common disposition for records that comprise a variety of material and media, including but not limited to demographic and financial data on individual borrowers; institutional data on schools, guarantors, lenders, private collection agencies; records of financial transactions, payment, collections, account balancing and reconciliation, and reporting; records pertaining to customer interactions; and related correspondence and documents.

As the records may be maintained in different media formats, this schedule is written to authorize the disposition of the records in any media (media neutral). Records that are designated for permanent retention and are created and maintained electronically will be transferred to NARA in an approved electronic format.

DISPOSITION INSTRUCTIONS:

a. Record Copy
   TEMPORARY
   - Cut off annually upon payment or discharge of loan. Destroy/delete 15 years after cut off.

b. Duplicate Copies Regardless of Medium Maintained for Reference Purposes and That Do No Serve as the Record Copy
   TEMPORARY
   - Destroy/delete when no longer needed for reference.

ELECTRONIC INFORMATION SYSTEMS:

Direct Loan Consolidation System (DLCS)
Total Permanent Disability System (TPD)
Debt Management and Collection System (DMCS)
Credit Management Data Mart (CMDM)

IMPLMENTATION GUIDEANCE:

Follow the disposition instructions in DoED 086 for system software; input/source record; output and reports; and system documentation. Original signed paper documents required for legal purposes must be kept for the full length of the retention period, even if an electronic version has been captured in the information system.

ARRANGEMENT/ANNUAL ACCUMULATION:

PREVIOUS DISPOSITION AUTHORITY:

SPECIFIC LEGAL REQUIREMENTS:

Title IV of the Higher Education Act (HEA) OF 1965, AS AMENDED

SPECIFIC RESTRICTIONS:
Privacy Act 18-11-05 Title IV Program Files
Privacy Act 18-11-08 Student Account Manager System

BUSINES LINE: Loans

Certifying Officials Signatures

_____ _____

Senior Program Official **Date**

_____ _____

Computer Security Officer/ Information System Security Officer **Date**

FOR SYSTEMS THAT COLLECT, MAINTAIN AND OR TRANSFER SSNS:

_____ _____

Assistant Secretary or designee **Date**

_____ _____

Kathleen Styles, Chief Privacy Officer **Date**