



**Privacy Impact Assessment**

**For**

ACS Education Servicing System (ACES)

**Date:**

**6/20/2011**

**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, [Brian.Sowl@Nelnet.net](mailto:Brian.Sowl@Nelnet.net)  
Nelnet Servicing, LLC  
Director Compliance and Vendor Management  
303.696.5278

**Office of Federal Student Aid  
U.S. Department of Education (ED)**

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) is used by ACS 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?

Titles II, IV-A, IV-B, IV-D, IV-E and V-C of the HEA (20 U.S.C. 1024, 1070a, 1070b-1070b-4, 1070c-1070c-4, 1070c-3a, 1071-1087-4, 1087a-1087j, and 1087aa-1087ii, and 1104 (1998); 31 U.S.C. Chapter 37). Higher Education Act of 1965 as amended §428 and §484(b)(4) and Code of Federal Regulations: 34 CFR §668 and §682

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 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.

ACES collects and maintains the following PII data pertaining to borrowers/co-borrowers/cosignors/students: full name, maiden name, Social Security Number (SSN), driver's license number and state, home street address, work street address, email address, home and work phone number, date of birth, loan number, bank account numbers, and other borrower information such as: disbursement amount, outstanding loan payment amount, monthly loan payment amount, loan status, forbearance status, deferment status, separation date, grace period, and delinquency status

The information is obtained from sources such as borrowers, students, co-borrowers, co-signors, educational institutions, lending institutions, other loan servicers, employers, references and external databases (e.g., Directory Assistance, National Change of Address (NCOA)).

Information is collected via the following channels: phone calls with ACS customer service agents, entries via the ACS Interactive Voice Response (IVR) service, incoming correspondence (e.g., via U.S. mail, email, etc.), entry via the Manage My Account borrower website, bulk file transfers from third-party data providers (e.g., Directory Assistance, National Student Clearinghouse), educational institutions and other loan servicers, as required, secure data transmission from ED applications such as the National Student Loan Data System (NSLDS) and the Debt Management Collection System (DMCS) and secure data transmission from the U.S. Department of Treasury (Treasury).

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.

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

The PII is necessary to properly service loans according to the regulatory requirements of Title IV servicing. The borrower name, address, email address, and phone numbers are essential for communicating with the borrower and performing collection activities. Endorser 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.

- The Nelnet Corporate Security Policy is in place which includes procedural, technological and physical controls to ensure required and necessary security protocols are continuously maintained.
- 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 segregation of duties.
- Associates are also required to complete a Security and 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.
- All security vulnerabilities are identified and track and mitigated thru 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.

The SSN is the unique identifier for Title IV programs and used 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, 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 Nelnet 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.

The HEA Act of 1965 and Privacy Act of 1974 provide the disclosure information.

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.

The internal uses to the information include fully satisfy all loan servicing and reporting requirements of Title IV programs and other applicable laws and regulations. This includes the following: verification of identity; determination of benefits, such as deferment, forbearance, discharge, or forgiveness; loan status reporting; location efforts for a skip borrower; and collection of a delinquent loan.

**7. Internal Sharing and Disclosure. Which internal ED 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 internal ED organizations this information is shared with include the National Student Loan Data System (NSLDS) and the Debt Management Collection System (DMCS).

The information shared is sensitive PII data student data and is shared for the purpose of fully satisfy all loan servicing and reporting requirements of Title IV programs and other applicable laws and regulations

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

The Department may disclose information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purposes for which the information in the record was collected. 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 computer matching agreements.

- (1) Program Disclosures
- (2) Feasibility Study Disclosure
- (3) Disclosure for Use by Other Law
- (4) Enforcement Disclosure.
- (5) Litigation and Alternative Dispute
- (6) Employment, Benefit, and Contracting Disclosure
- (7) Employee Grievance, Complaint or Conduct Disclosure
- (8) Labor Organization Disclosure.
- (9) Freedom of Information Act
- (10) Disclosure to the DOJ
- (11) Contract Disclosure
- (12) Research Disclosure
- (13) Congressional Member Disclosure
- (14) Disclosure to OMB for Credit Reform Act (CRA) Support

The system shares information with the following external entities: U.S. Department of Treasury (Treasury), Internal Revenue Service, (IRS), institutions of higher education, national credit bureaus, lenders, and servicers.

PII is shared for the purpose of servicing 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.

The information sharing is pursuant to MOU's and ISA's and have been authorized and approved prior to sharing data with these external entities.

Nelnet Servicing, LLC has Memorandums of Understanding (MOU) and Interconnection Security Agreement (ISA) with the Department of Treasury Financial Management Services (FMS), CoSentry, Fiserv and Iron Mountain.

**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?

Individuals are provided with a notice as required by the Privacy Act of 1974 as part of the promissory note materials. The notice explains what types of PII is being collected, why it's being collected and how it will be used. The Privacy Act provides the individual the ability to access their account and the right to request an amendment of an y inaccurate information in their record.

Individuals are provided with the Department of Education's privacy policy in accordance with the Gramm-Leach-Bliley Act (GLBA), and annually thereafter.

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

The Nelnet Servicing, LLC privacy policy will be available on [www.Nelnet.com](http://www.Nelnet.com).

**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?

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

Nelnet 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.
- Nelnet physically allocates 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 ED data access is available to authorized and approved users with a 5C or 6C security clearance with the exception of information access by individual borrowers through Manage My Account (MMA).
- Privileged access to ACES is limited to only 6C security cleared personnel.
- Signed Rules of Behavior and Security Awareness training for all employees.
- OMB Clearances
- System required User IDs and passwords
- Annual auditing and continuous monitoring

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 System of Records Notice, Common Services for Borrowers (CSB) Contract, 18-11-16, 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:

Records are covered under ED 072 FSA Application, Origination and Disbursement Records, Nara Disposition Authority N1-441-09-23. Cut off annually upon end of application cycle year. Destroy/delete 15 years after final repayment or audit of student financial obligation, or after student record information is transferred to alternate recordkeeping system (i.e., loan servicing system), whichever is sooner.