Privacy Impact Assessment
For
Not-for-Profit Oklahoma Student Loan Authority (NFPOSLA)

Date:
May 15, 2012

Point of Contact:
Tammy Morton
202-377-4653
Tammy.Morton@ed.gov

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

Author:
Ann Cole
405-556-9273
ACole@osla.org

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 Not for Profit Oklahoma Student Loan Authority (NFPOSLA) system is used by the Oklahoma Student Loan Authority (OSLA) to service Federal Student Aid (FSA) Title IV student loans. The operational capabilities include borrower account management, loan conversion/de-conversion, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, claims and correspondence history files updates and collection and skip tracing.

   The NFPOSLA system communicates with the internal FSA platforms, borrowers, 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 U.S. mail, telephone calls, a secure borrower website, secure 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 NFPOSLA 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 the Manage My Account function.

   NFPOSLA collects and maintains the following PII data pertaining to borrowers, co-borrowers, co-signors or students:

   - Full name
   - Maiden name
   - Social Security Number (SSN)
   - Bank account numbers
   - Student Loan account number
   - Driver's license number and state
   - Alien registration number
   - Date of birth
   - Home address
   - Related demographic data
   - Home, work, alternate, mobile telephone number
   - Financial information

- Email address
- Employment information
- Medical information (to the extent required for purposes of certain deferments and discharge requests)
- 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 status.

The information is obtained from sources such as borrowers, students, co-borrowers, co-signors, educational institutions, lending institutions, employers, references and external databases (e.g., Directory Assistance).

Information is collected via the following channels:

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 Department of Education (DoED) 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 any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were m The information is necessary to the mission of OSLA in order to comply with the Higher Education Act (HEA) policies, regulations and statues.**

   The PII is necessary to properly service loans according to the regulatory requirements of the HEA. 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 OSLA Information Security Policy is in place which includes procedural, technological and physical controls to ensure required and necessary security protocols are continuously maintained.
   - OSLA staff with the ability to access this information requires a government 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.
   - OSLA staff is also required to complete a Security and Awareness Training annually.
   - Annual risk assessments are performed.
   - All OSLA staff must comply with security policies and procedures, and will report security problems or incidents to the OSLA Security Team.

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 HEA 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 DoED, Internal Revenue Service, institutions of higher education, national credit bureaus, and servicers.

Borrowers (and endorsers, if applicable) are advised of the collection and use of the SSN in the promissory note materials of their HEA 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.

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 information is collected and maintained to enable NFPOSLA to perform Federal Student Aid business related to student loans and is necessary to adequately service and ensure successful collection of loans. The NFPOSLA system will employ the information to support the following capabilities:

- Support for its Federal Student Aid student loan servicing function. Operational capabilities include loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, collection, skip-tracing, and correspondence history files.
- Provide three major forms of account management and customer access for borrowers. The NFPOSLA system currently provides a secure website where the borrower can access account information and conduct specific loan transactions. The borrower can also place calls for self service via the IVR or to live customer service agents where the full range of loan services is provided. Finally, the borrower can also mail in forms and other correspondence to the NFPOSLA system.
- External uses of the information include:
    - Reporting to consumer reporting agencies for purposes of credit reporting
    - Reporting to Directory Assistance to verify telephone numbers
    - Exchanging information held by the NSC and educational institutions for purposes of educational data and address verification
    - Exchanging information held by the U.S. Postal database for purposes of checking the validity of zip codes entered and validating address updates
    - Exchanging information with skip-trace vendors for purposes of verifying/obtaining updated borrower contact information
    - Exchanging information with tax assessor offices for purposes of verifying/obtaining updated borrower contact information

- Providing information to NSLDS, which is used by educational institutions for purposes of determining eligibility for programs and benefits
- Exchanging information with person locator services which may be used during skip-tracing and collections activities in order to locate the borrower or collect payments

The data can be analyzed by system processes and by NFPOSLA employees. Specific methods used include manual calculations and analysis of data using desktop query tools and SAS.

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?**

In accordance with requirements set forth by DoED, the NFPOSLA system shares information with DoED to allow it to administer the Direct Loan Program. DoED may disclose information contained in a record in an individual's account in accordance with the Privacy Act of 1974. NFPOSLA shares information with:

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

Please refer to Section 4, which describes what information is shared, for what purpose the information is shared, and the risks to privacy for internal sharing and disclosure as well as how the risks are mitigated.

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?**

NFPOSLA will be required to interface and share information with the following non-Department of Education systems and government entities:

- Internal Revenue Service, (including Adjusted Gross Income requests, waiver image processing, and 1098E/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 (to obtain updated contact information).

NFPOSLA may be required to interface and share information with the following non-governmental entities:

- Educational institutions (to coordinate the management of the loan with the educational institution's financial aid office)
- Direct Loan servicers, and other servicers (in connection with conversion or de-conversion of loans to/from the NFPOSLA system)
- Independent auditors (SSAE16, FSA auditors)
- National consumer reporting agencies (to obtain updated contact information and enrollment status)
- Person locator services (to obtain updated contact information)
- Other parties as authorized by the borrower (employers, references)
- NCOA (to obtain updated mailing address information)
- Optional support vendors (to provide services to the NFPOSLA system in connection with NFPOSLA servicing of DoED loans)

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, and correspondence history files.

The information sharing is pursuant to Memoranda of Understanding (MOU's) and Interconnection Security Agreement (ISA's) and has been authorized and approved prior to sharing data with these external entities.

9. Notice. Is 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-BlileyAct, 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 NFPOSLA's secure borrower portal website (www.osla.org) and
- In order to establish an online account on the NFPOSLA system secure borrower portal website, the borrower must agree to the Terms 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 OSLA through its secure borrower Web site 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 NFPOSLA system, such as paperless document delivery and online payment services.

OSLA 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.

www.osla.org/PrivacySecurity.aspx

www.fasfa.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 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.

OSLA 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 NFPOSLA.

OSLA 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 NFPOSLA is limited to only 6C security cleared personnel.
- Signed rules of behavior and security awareness and privacy training for all employees.
- Government clearances
- System required User IDs and passwords
- Annual auditing and continuous monitoring
- Two Factor Authentication (TFA) has been implemented at OSLA and is employed to ensure the identity of the users of its system.

The OSLA System Security Plan (SSP) details the security requirements and describes the security controls that are in place to meet those requirements.

Security authorization will be completed June 20, 2012.

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

- Federal Information Security Controls Audit Manual (FISCAM)
- Federal Information Processing Standards Publications (FIPS 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 Firewall 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 Systems, 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 800-60, Rev. 1, Volume 2, Appendices to 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, Integrating IT Security into the Capital Planning and Investment Control Process. January 2005
- NIST SP 800-70, Rev. 2, National Checklist Program for 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 Procedures
- 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?**

NFPOSLA is covered under the following System of Records Notice: “Common Services for Borrowers (CSB)”, 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, NFPOSLA will follow the FSA Loan Servicing, Consolidation, and Collections Records. 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, consolidation of direct loans, managing and recovering defaulted debts assigned to the Department from Federal Family Education Loan (FFEL) and other lenders, rehabilitated loans, and any other type of Title IV student aid obligation.

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, payments, collections, account balancing and reconciliation, and reporting; records pertaining to customer interactions; and related correspondence and documents.

As these 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 Not Serve as the Record Copy
   TEMPORARY
   - Destroy/delete when no longer needed for reference.

ELECTRONIC INFORMATION SYSTEMS:
Direct Loan Servicing System (DLSS)
Direct Loan Consolidation System (DLCS)
Conditional Disability Discharge Tracking System (CDDTS)
Debt Management and Collection System (DMCS)
Credit Management Data Mart (CMDM)

IMPLEMENTATION GUIDANCE:
Follow the disposition instructions in DoED 086 for system software; input/source records; 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
BUSINESS LINE: Loans