Privacy Impact Assessment

For:
Not-For-Profit Missouri Higher Education Loan Authority (NFPMOHELA)
Missouri Higher Education Loan Authority (MOHELA) Commercial System

Date:
May 17, 2012

Point of Contact:
Gregory Plenty
(202) 377-3253
Gregory.Plenty@ed.gov

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

Author:
Don Bertier
(636) 532-0600
donb@mohela.com

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.**

System Name	Systems Acronym	Description of Commercial Systems
MOHELA Commercial Systems	NFPMOHELA	The NFPMOHELA system provides ancillary services required to service the Department's assets.

The Missouri Higher Education Loan Authority Computer System, operated by the Pennsylvania Higher Education Assistance Authority (PHEAA), and hereafter referred to as Not For Profit MOHELA (NFPMOHELA), is a network of support systems that retrieve, store and present information throughout the system. The purpose of the system is to support the primary activities and operations required to service Federal Student Aid (FSA) Title IV student loan assets. The system is composed of a loan servicing system, interfaces, and auxiliary systems, which include the following major functional components:

- Internet Website - Provides access to public and non-public information based on account access
- Financial Management System (FMS) – Provides reconciliation and reporting to Federal Student Aid's (FSA's) FMS using the Sage MAS 500 financial accounting system
- Mailstream System – Provides fulfillment processes to route, distribute, configure, print, reprint, and report mail correspondence
- Telecom Systems – Provides a Voice Response Unit system for borrower self-service options, auto-dialer for making outbound calls, call recording, and call management for monitoring contact center performance and activity
- Imaging System – Provides storage and access to incoming borrower correspondence.
- Asset Acquisition and Conversions – Provides functionality for loading loans onto the servicing system. Loans can be received from origination or consolidation systems and from external sources when loans are purchased or originated in an external platform
- Common Modules – Provides functionality that is shared or used by other parts of the system. This includes person and institution demographics, account number assignment, correspondence, activity logging, queuing, loan archiving, and other functionality. These shared components allow for isolation of repetitive business logic and ease of maintenance
- Consumer Reporting Agency Reporting – Produces the required transmissions for communicating with consumer reporting agencies
- Letter Writer – Supports the definition, composition and printing of all outgoing letters. This includes both automated system-generated letters and ad-hoc communications
- Loan Program Definition – Supports and maintains system parameters that provide flexibility in all aspects of student loan servicing
- Loan Servicing – Provides functionality for all aspects of the day-to-day servicing of student loans. This includes account maintenance, repayment schedules, billing, payment processing, deferment/forbearance processing, interest capitalization, borrower benefits, account adjustments and paid-in-full processing
- Manifest – Reports loan information to the National Student Loan Data System (NSLDS)
- Social Security Number (SSN) Change – Provides the ability to correct social security numbers on the servicing system

- Tax Reporting – Produces federally required 1098-E and 1099-C tax reports to both the borrower and Internal Revenue Service (IRS)
- Page Center – Provides electronic document delivery, both internally and to clients. PageCenter controls the creation of all production output for viewing, long-term retention and printing. In most cases, output is placed into PageCenter from batch production Job Control Language (JCL) containing unique class, writer and destination codes. All data resides on the mainframe.

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, Title IV, 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 NFPMOHELA 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), 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 the U.S. Department of the 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 NFPMOHELA databases and PHEAA 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.**

   This information is collected to meet the contractual requirements of Federal Student Aid, enabling MOHELA to perform student loan servicing activities. This information is necessary to uniquely identify borrowers for purposes of meeting the contractual requirements to service Federal student loans on behalf of Federal Student Aid.

   Privacy risks would result from a breach of MOHELA's security safeguards as implemented on the NFPMOHELA system or Pennsylvania Higher Education Assistance Authority (PHEAA's) security safeguards as implemented on the PHEAA system, which could compromise the confidentiality, integrity and availability of information. The most likely method of breach would be through unauthorized system access that would enable an adversary to disclose, damage the integrity of, or prevent the availability of information.

   Physical security, such as access badges and security cameras protect against unauthorized access to component facilities. Unauthorized access to systems is addressed by network intrusion detection systems, firewall log monitoring, and malware detection and correction software. To prevent unauthorized use of systems by employees, audit logs are kept and checked at regular intervals and access to systems is restricted by limiting access based on the principle of least privilege. Unauthorized system use by employees is subject to disciplinary action. Annual security training is required for all employees. Additional information regarding risk mitigation and security safeguards is provided in Question 11 hereof.

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 collected as required for participation in Federal student loan programs. The SSN is the unique identifier for Title IV student loan 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 Federal laws and regulations. Trading partners include the Department of Education, Internal Revenue Service, and institutions of higher education, nationwide consumer reporting agencies, and servicers.

   Subsequent collection of SSNs as required on federal forms, by phone, or on the website; is used for verification purposes only. The SSN is used to communicate with authorized entities such as the Department of Education, IRS, educational institutions, consumer reporting agencies and person locator services.

   The system assigns a unique account number to each borrower that is used to communicate with the borrower and whenever possible in lieu of the SSN, to avoid unnecessary disclosure of SSN's. Borrowers who exercise their option to use the NFPMOHELA website are required to create a unique user ID that does not match their SSN.

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 MOHELA 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 the 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 the PHEAA system for the 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?**

   As required by NFP-RFP-2010, information will be shared with Federal Student Aid and its agents and contractors:

   - Federal Student Aid and its agents or Contractors
   - National Student Loan Data System (NSLDS)
   - Debt Management Collection System (DMCS2)
   - 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 NFPMOHELA 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 request, 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. 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-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 NFPMOHELA's secure borrower portal website (www.mohela.com)
- In order to establish an online account on the NFPMOHELA 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 the MOHELA 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 NFPMOHELA system, such as paperless document delivery and online payment services.

MOHELA 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.mohela.com

www.fafsa.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?

MOHELA employs administrative, technical, and physical security controls of its facilities and systems in accordance with the Federal Information Security Management Act (FISMA).

MOHELA has implemented the following groups of technical and operational controls:

- Access Control – System and information access security utilizes a variety of network-based measures including, but not limited to, centralized active directory management, firewalls, secure connections, encryption, remote access Virtual Private Networks (VPNs) and password policy enforcement (including strength, rotation, etc.).
- Two Factor Authentication-Two Factor Authentication (TFA) is not yet implemented on NFPMOHELA yet. It will be implemented on this system later this year.
- Password Policy – MOHELA's password policy includes:
    - Verifies as part of the initial password distribution, the identity of the individual and/or devices receiving the password
    - Initial passwords distributed by the help desk to the user must conform to MOHELA password policies
    - Requires that for initial password distribution, for lost/compromised or damaged passwords, and for revoking passwords be distributed by the help desk to the supervisor to the user in an email or phone call

  - Requires complex password content, password strength, frequency for changing or refreshing passwords, the minimum and maximum lifetime restrictions, and reuse conditions
  - Establishes minimum and maximum lifetime restrictions and reuse conditions for authenticators
  - Requires that passwords be changed every 60 days for user accounts and as required for service accounts or machine IDs. Service accounts or machine IDs are for accounts that are used in system processes and are not subject to human interaction
  - Requires protection of authenticator content from unauthorized disclosure and modification
  - Requires that default passwords of information system components be changed upon installation of the components
  - Security Awareness training includes instructions in measures to safeguard passwords from unauthorized disclosure
  - Requires passwords to be encrypted at rest and masked when displayed on a screen.
- Integrity and Availability – Operating policies include regular vulnerability scans, security and patch updates, backup and operations redundancy/failover facilities, secure disposal of key operating assets as well as physical and environmental protection.
- Security Clearance and Awareness – All MOHELA personnel are required to obtain a 5C or 6C government security clearance and complete Security Training and Awareness course as well as annual refresher training.
- Security and Contingency Plans – MOHELA maintains a Configuration Management Plan, Contingency Plan and Incident Response Plan covering equipment, personnel and procedures.

The NFPMOHELA system has been Authorized to Operate by FSA. It was authorized on January 18, 2012.

The NFPMOHELA 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?**

NFPMOHELA is covered under the "Common Services for Borrowers" System of Records 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, NFPMOHELA 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

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**