Privacy Impact Assessment
For
PHCS
PHEAA FEDERAL LOAN SERVICING SYSTEM (FLS)

Date:
August 21, 2009

Point of contact:
Matthew Sessa
Program Director
717-720-2248
msessa@pheaa.org

System Owner:
Terri Slocomb
VP, Application Development
717-720-3875
tslocomb@pheaa.org

Author:
Jody L. W. Angelini
VP, Enterprise Security Office
717-720-3337
jangelin@pheaa.org

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

Expiration Date: September 1, 2010

1. **System Information. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.**

Information System Name and Identifier	PHEAA Acronym	Federal Acronym
Federal Loan Servicing System	FLS	PHCS

PHEAA's Federal Loan Servicing (FLS) System is a mainframe-based decision support tool comprised of modules that store information in tables and make the information available as needed throughout the system. The FLS System purpose is to support the management and servicing of federal student loan programs throughout the entire loan lifecycle.

The FLS System is comprised of a core mainframe application, a mainframe database, a web-based customer facing interface and other auxiliary systems, and includes the following major functional components:

a. Asset Acquisition and Conversions - Provides functionality for loading loans onto the servicing system. Loans can be received from our Origination or Consolidation systems and also from external sources when loans are purchased or originated in an external platform.

b. Automated Calling Process - Supports functionality for extracting and loading loans to the auto-dialer for queuing and processing outbound calls. Also used for processing and notating inbound calls.

c. Automated Loan Sales - Provides functionality for scheduling and processing loan sales between owners.

d. Common Account Maintenance - Supports the communication of loan status change information with guarantors that accept the CAM format.

e. 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.

f. Consumer Reporting Agency Reporting - Produces the required transmissions for communicating with consumer reporting agencies.

g. Due Diligence - Supports processing associated with performing due diligence on delinquent loans, as well as claim, pre-claim, cure, litigation and skiptrace processing.

h. Interactive Voice Response System - Supports the automated response to incoming borrower phone calls requesting account information.

i. Letter Writer - Supports the definition, composition and printing of all outgoing letters. This includes both automated system-generated letters and ad-hoc communications.

j. Loan Program Definition - Supports and maintains system parameters that provide flexibility in all aspects of student loan servicing. Parameters can be defined at the guarantor, loan program, regulatory category and owner levels (among others) and can be used to define and direct system processing for all aspects of student loan origination and servicing.

k. 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.

l. Manifest - Reports loan information to non-CAM compliant clients and to the National Student Loan Data System (NSLDS).

m. SSN Change - Provides the ability to correct social security numbers on the FLS System.

n. Tax Reporting - Produces federally required 1098-E and 1099-C tax reports to both the borrower and Internal Revenue Service ("IRS").

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?

3. **Characterization of the Information.**

3.1 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.)?

The FLS System collects and maintains the following elements of PII:

- Full Name
- Address
- Social Security Number
- Telephone Number
- 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.

3.2 What are the sources of information (e.g., student, teacher, employee, university)?

Information is provided by the applicant/borrower, references provided by the borrower, educational institutions, financial institutions, the U.S. Department of Education, NSLDS, National Student Clearinghouse, and other parties that may provide documentation for the servicing of student loans, such as the U.S. military, commercial person locator services, national consumer reporting agencies, and the U.S. Department of the Treasury.

3.3 How is the information collected (website, paper form, on-line form)?

Paper form, website, on-line form, electronic data transmission, and telephone.

3.4 Is the information used to link or cross-reference multiple databases?

Yes. The information is used to link or cross-reference multiple internal (PHEAA) databases.

Web Databases. These are updated, not read only. This data does not exist on the mainframe. Houses data needed to meet needs for reporting on web access. IVR & OPS tables house information for use by our dialer software, containing borrower and loan information and is used to record results. Deferment & Forbearance is used to allow borrowers to apply on-line for deferments and forbearances, recording the results.

PeopleSoft. Houses data for Agent Effectiveness for our Loan Servicing Center.

DataMart. Servicing aggregate data used as a Decision Support System and an Executive Information System supporting informational and analytical needs.

Data Warehouse (Servicing Data). The FLS Data Warehouse is used to support the FLS System as a Decision Support System and an Executive Information System that supports informational and analytical needs by providing integrated and transformed enterprise-wide historical data for management analysis and reporting. The Data Warehouse is a read-only, integrated database designed to answer comparative and "what if" questions. Unlike operational databases that are set up to handle transactions, data warehouses are analytical, subject-oriented and are structured to aggregate transactions as a snapshot in time.

Imaging System. The Imaging System allows for intelligent business process workflow routing and archive search and retrieval capability of electronic loan servicing documents. The system provides disaster recovery, accessibility, scalability, security, error reduction, automation, speed, and efficiency to historically human and paper centric processes.

PageCenter. System is used for 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 JCL containing unique class, writer and destination codes. All data resides on the mainframe.

4. **Why is the information collected?**

This information is collected to enable PHEAA to perform Federal Student Aid business related to student loans. PHEAA's FLS System supports Federal Student Aid in servicing student loans.

4.1 How is this information necessary to the mission of the program, or contributes to a necessary agency activity.

This information is necessary to identify borrowers and to service their student loans on behalf of Federal Student Aid. The FLS System database assists in tracking information pertinent to the borrower as well as information needed to process and service student loans throughout the loan life cycle. Collection of this information protects Federal Student Aid's fiscal interest by supporting timely and full repayment of loans and enables PHEAA to assist borrowers with managing their loans. The information is also needed to determine borrower eligibility for entitlements such as deferments, forbearances, and discharges, and to locate borrowers in cases of invalid addresses and/or phone numbers.

4.2 Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks would result from a breach of PHEAA's security safeguards as implemented on the FLS 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.

The risk of data compromise is mitigated by several steps. Physical security, such as guards, access badges and security cameras protect against unauthorized access to component facilities. Unauthorized access to the system itself is addressed by network intrusion detection systems, firewall log monitoring, and malware detection and correction software. To prevent unauthorized use of the FLS System by PHEAA employees, audit logs are kept and checked at regular intervals and FLS System access is restricted by limiting access based on the principle of least privilege. Unauthorized system use by PHEAA employees is subject to strict penalties. PHEAA requires annual security training for all employees and implements security controls as mandated in Security Requirements for Federal Information and Information Systems, and Recommended Security Controls for Federal Information Systems. Implementation of these controls and associated risks and mitigation is reflected in required security documentation. Additional information regarding risk mitigation and security safeguards is provided in Section 11.1.

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.**

Collection of applicant/borrower SSN is required for participation in Federal student loan programs. The SSN is collected on various federal forms, such as the Master Promissory Note (MPN) and deferment and discharge forms. PHEAA assigns an account number to each borrower that is used to communicate with the borrower in lieu of the SSN. We use the SSN to communicate with the Department of Education and educational institutions, and as otherwise may be required to

service student loans. The SSN is also contained in data transmitted to consumer reporting agencies and person locator services.

6. Uses of the Information.

6.1 What is the intended use of the information?

The information is collected and maintained to enable PHEAA to perform Federal Student Aid business related to student loans and is necessary to adequately service and ensure successful collection of the loans.

6.2 How will the information be used?

The information is necessary to identify borrowers and to manage Federal Student Aid's student loan portfolio. The FLS System database assists in tracking information pertinent to the borrower as well as information needed to process and adequately service student loans throughout the repayment period. Collection of this information protects Federal Student Aid's fiscal interest by supporting timely and full repayment of loans, and enables PHEAA to assist borrowers with managing their loans. The information is also used to determine borrower eligibility for entitlements such as deferments, forbearances, and discharges, and to locate borrowers in cases of invalid addresses and/or phone numbers.

6.3 Describe all internal and/or external uses of the information.

The information in the FLS System database assists in the tracking of information pertinent to borrowers' student loans. The information enables PHEAA to properly service the loans and to assist borrowers throughout their repayment period. The information is used to collect payments from borrowers, to prevent default, to determine eligibility for entitlements such as deferments, forbearances, and discharges, and to locate borrowers in cases of invalid demographic information.

External uses of the information include reporting to consumer reporting agencies for purposes of credit reporting and providing information to NSLDS, which is used by educational institutions for purposes of determining eligibility for programs and benefits.

6.4 What types of methods are used to analyze the data?

The data can be analyzed by system processes and by PHEAA employees. Specific methods used include manual calculations and analysis of data using desktop query tools and SAS which, are run both against the production environment and in the data warehouse, as well as regularly scheduled automated processes.

6.5 Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

This information will be used as set forth in Sections 6.2 and 6.3. The primary sources of information will be various Federal agency databases, as well as lenders and servicers from whom the Department of Education purchases student loans. Information may also be obtained from

person locator services and consumer reporting agencies, and may be used during skip tracing and collections activities in order to locate the borrower and collect payments.

7. Internal Sharing and Disclosure.

7.1 With which internal DoED organizations will the information being shared?

Federal Student Aid and its agents or contractors:

- Financial Management System (FMS)
- National Student Loan Data System (NSLDS)
- Debt Management Collection System (DMCS)
- Conditional Disability Discharge Tracking System (CDDTS)
- Post Secondary Education Participant System (PEPS)
- Common Origination and Disbursement System (COD) - (including eMPN and TEACH GRANTS)
- Student Aid Internet Gateway (SAIG)
- Common Services for Borrowers (CSB) DataMart or future datamarts, optional
- eCampus Based, future
- National Student Clearinghouse

7.2 *What information is shared?*

All information described in Section 3.1 hereof may be shared.

7.3 *For what purpose is the information shared?*

The information is only shared as required to complete Federal Student Aid business related to the student loans.

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

See response to Section 4.2 hereof.

8. External Sharing and Disclosure.

8.1 With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)?

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

- IRS, (including AGI income request, waiver image processing and 1098/1099)
- U.S. Department of Treasury ("Treasury") (including Lockbox, EDA vendor, Pay.gov, Remittance Express, IPAC, and, Ca$hLinkII)
- United States Postal Service

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

- Educational Institutions
- Guaranty Agencies
- Lenders, Lender Servicers, Direct Loan Servicer, and other Servicers
- Independent Auditors
- National Consumer Reporting Agencies
- Person Locator Services
- Other parties as authorized by the borrower

8.2 What information is shared?

All information described in Section 3.1 hereof may be shared.

8.3 For what purpose is the information shared?

The information is only shared as required to complete Federal Student Aid business related to the student loans.

8.4 How is the information shared outside of the Department?

Information shared outside of the Department of Education is shared through secure file transmissions and secure email.

8.5 Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency?

Sharing of information with Federal government agencies will be pursuant to an MOU or ISA, and/or pursuant to other contractual or regulatory requirements. Sharing of information with certain other 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.

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

See response to Section 4.2 hereof. Additionally:

- All information is protected by multi-factor authentication and monitored by automated and manual controls.
- Data is housed within a secure facility and controlled by PHEAA.
- All data is encrypted or otherwise secured, as appropriate, as it moves between PHEAA and ED systems, government systems, schools, guaranty agencies, lenders, servicers, independent auditors, private collection agencies, national consumer reporting agencies, the United States Postal Service, and person locator services.

9. Notice.

9.1 Is a notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)?

Yes. We will send the following written Privacy Notice provided by FSA to borrowers when they initially convert to the FLS System and annually thereafter:

> In 1999, Congress enacted the Gramm-Leach-Bliley Act (Public Law 106-102). This Act requires that lenders provide certain information to their customers regarding the collection and use of nonpublic personal information. Because you have a loan held by the U.S. Department of Education, we are sending you this Notice. In general, the categories of nonpublic personal information collected about you from your application, your educational institution, and consumer reporting agencies, include your address and other contact information, demographic background, loan and educational status, family income, social security number, employment information, collection and repayment history, and credit history. We disclose nonpublic personal information to third parties as necessary to process and service your loan and as permitted by the Privacy Act of 1974. The Privacy Act permits disclosure to third parties as authorized under certain routine uses. Examples of disclosures permitted under the Privacy Act include disclosure to federal and state agencies, private parties such as relatives, present and former employers, and creditors, and our contractors for purposes of administration of the student financial assistance programs, for enforcement purposes, for litigation, and for use in connection with audits or other investigations. We do not sell or otherwise make available any information about you to any third parties for marketing purposes. We protect the security and confidentiality of nonpublic personal information by implementing the following policies and practices. All physical access to the sites where nonpublic personal information is maintained is controlled and monitored by security personnel. Our computer systems offer a high degree of resistance to tampering and circumvention. These systems limit data access to our staff and contract staff on a .need-to-know basis, and control individual users' ability to access and alter records within the systems. All users of these systems are given a unique user ID with personal identifiers. All interactions by individual users with the systems are recorded.

9.2 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?

We will apply the Department of Education's privacy policy and comply with applicable Federal and state law. Borrowers are able to opt out of our online account access features, and are required to provide consent, in compliance with applicable law, for various features and services provided by the FLS System, such as paperless billing, online payment, and telephone payment services.

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

There are Privacy Act Notices on the PHEAA System and its legacy sites for both internal and external users, including public users. The following link is representative of the Privacy Act Notice: http://www.myfedloan.org/about/privacy-policy.shtml

In addition, there is a Privacy Act Notice on the PHEAA Mainframe for the FLS System: The following is posted on the application's login page:

WARNING: This is a Department of Education computer system. Department of Education computer systems are provided for the processing of Official U.S. Government information only. All data contained on Department of Education computer systems is owned by the Department of Education and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.

THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM.

System personnel may give to law enforcement officials any potential evidence of crime found on Department of Education computer systems. Unauthorized use of this system is a violation of Federal law and can be punished with fines or imprisonment (P.L. 99-474).

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.

11. Security.

11.1 What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc.

PHEAA develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

All policies and procedures may be found on PHEAA's internal website at: http://nereids/policy/index.jsp. PHEAA provides comments on policies and procedures through the Vigilant Policy Center application.

Application IDs are reviewed by the Enterprise Security Office (ESO) quarterly. The ESO provides a list of current users to business points of contact and requests them to verify who has left each project or no longer needs access to each application. The ESO removes access as appropriate. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. Authorized users of the information system are identified and provided specific access rights/privileges. System access is granted based on: (i) a need-to-know, determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage.

Proper identification is required prior to establishing or approving information system accounts. All use of guest/anonymous accounts is specifically authorized and monitored, and unnecessary accounts are removed, disabled, or otherwise secured. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

Information is secured following the guidance of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, Computer Security Act of 1987. In addition, PHEAA is currently preparing the System Security Plan (SSP) that details the security requirements and describes the security controls that are in place to meet those requirements. A certification and accreditation process in accordance with the National Institute of Standards & Technology (NIST) Guide for the Security Certification and Accreditation of Federal Information Systems will validate our security controls.

PHEAA's placement of network protection mechanisms, procedures and policies is intended to increase the dependability of our IT systems where multiple layers of defense prevent espionage and direct attacks against critical systems. PHEAA's network security is based on the principle of Defense in Depth. Defense in Depth is a security strategy pursuant to which network defenses are layered so that a breach in one layer only leads the attacker to the next layer of defensive countermeasures. Layering our network defenses helps prevent direct attacks against critical systems and data, increases the likelihood of an attacker being detected, and gives PHEAA more time to realign defenses to where they are most needed in the event of an actual, ongoing attack, reducing and mitigating the impact of a breach. PHEAA's network mechanisms consist of the following:

- Intrusion Detection System (IDS): Network-Based IDS, Host-Based IDS, and Application-Based IDS
- Firewall and Routers: Packet Filtering, Proxy Server, and Stateful Packet Filtering
- Virtual Private Network (VPN): IPSec VPN and SSL VPN
- Secure Configuration of Operating Systems: Deactivation of unnecessary network services, Authentication and password security, Restrictive granting of rights, Enforcement of strict account policies, Audit logs, Anti-Virus, Continuous Vulnerability Scans, and Formalized Patch Management Process
- Network Policies and Procedures: Staff Training, Security Update Plan, Contingency Plan, and Vulnerability Analysis Tools

PHEAA uses software to monitor, notify and block malicious attacks 24/7. If unusual or suspicious activity is detected, ESO personnel are notified via cell phone alerts.

PHEAA contracts with Verizon (CyberTrust) to examine, measure, and validate our security controls, policies, and procedures against a stringent set of Essential Practices defined by Verizon (CyberTrust).

Physical access to PHEAA facilities is secured by a computer-based networked security system, which is maintained by PHEAA and supported by an outside security company. Individually programmed photo ID access cards enable associates to access buildings and secure areas as

authorized by their manager and the authority that approves access to restricted areas. Secured areas, such as the data center, require an access badge and PIN number to gain access. Armed contract security officers patrol PHEAA facilities. Video images from all cameras are continuously captured and digitally recorded and stored for thirty days. The ESO generates quarterly access review reports, which are distributed to the authorities who approve restricted area access. These authorities review the lists to ensure access is granted only to those who are authorized.

Visitors entering PHEAA facilities must provide a valid form of photo identification and sign in and out using the visitor log at the security desk. Visitors are escorted from the security desk to and from their destination by the business unit they are visiting.

11.2Has a Certification and Accreditation (C&A) been completed?

No. We are currently in the process, and FSA is expected to be on-site to conduct an audit in November 2009

11.3Is the system compliant with any federal security requirements? If so, which federal security requirements?

Federal Standards and Guidelines

- 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, November 2001
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, January 2002
- NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-35 Guide to Information Technology Security Services, October 2003
- NIST SP 800-37 Information Technology Certification and Accreditation Guide, October 2003
- NIST SP 800-40 Procedures for Handling Security Patches, August 2002
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- NIST SP 800-42 Guidelines on Network Security Testing, October 2003
- NIST SP 800-44 Guidelines on Securing Public Web Servers, September 2002
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002
- NIST SP 800-50 Building an Information Technology Security Awareness Program, 2nd Draft, April 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, October 2003
- NIST Draft Special Publication 800-53, Revision 1 (Final Public Draft), October, 2006, Recommended Security Controls for Federal Information Systems

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?

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:

    Yes. The Department of Education has provided the following ED Records Schedule:
    ACS Tracking Number: OM:6-0106:L74

Signatures on Following Page

The parties hereto acknowledge that Section 2 and Section 12 of this Privacy Impact Assessment are incomplete as of the execution hereof. Information for these Sections will be provided at a later date.

Certifying Officials Signatures:

Helen Shumate — 8/31/09

System Owner — **Date**

Program Office Computer Security Officer — **Date**

For systems that collect, maintain and or transfer SSNs:

Senior Program Official — **Date**