Privacy Impact Assessment

For

Cornerstone℠ System

Date:

December 2, 2011

Point of Contact:

Tammy Morton, (202) 377-4653, Tammy.Morton@ed.gov

System Owner:

Keith Wilson, (202) 377-3591, Keith.Wilson@ed.gov

Author:

Angela Duff, 801-321-7266, aduff@utahsbr.edu

Office of 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.

Information System Name	System Acronym
Cornerstone[SM] System	NFP-Utah

Purpose
The Cornerstone[SM] System is an integrated decision support system. The operational functionality includes borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, collections, skip-tracing, discharge processing and correspondence history files.

The Cornerstone[SM] System supports the servicing and management of all types of Title IV student financial aid obligations throughout the entire loan lifecycle. The Cornerstone[SM] System also communicates with the internal Federal Student Aid (FSA) platforms, borrowers, educational institutions, other loan servicers, third-party data providers, consumer reporting agencies, and government agencies (as permitted by the Privacy Act of 1974). Channels of communication include mail, phone calls, a secure borrower Web Site, e-mail and secure data transfer links.

Scope
The major system components of the Cornerstone[SM] System are hosted with Pennsylvania Higher Education Assistance Agency (PHEAA). These major system components consist of a core mainframe application, a mainframe database, a web-based customer facing interface and other auxiliary systems. This system, which is maintained in Harrisburg, PA, is an official system of records under the Privacy Act.

Other auxiliary systems, maintained at the Utah Higher Education Assistance Agency (UHEAA) facility in Salt Lake City, UT, interconnect with the PHEAA major system components. These auxiliary systems are comprised of a Customer Service user interface, interactive voice response (IVR), autodialer, imaging system, e-mail servers, and databases.

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 Cornerstone[SM] System acts as a component of the broader U.S. Department of Education/Federal Student Aid loan servicing solution, which derives its legal authority to collect and use the information from and about the borrower from §§421 et seq. of the Higher Education Act (HEA) of 1965, as amended (20 U.S.C. 1071 et seq.), and the authorities for collecting and using the borrower's Social Security Number (SSN) are §§428B(f) and 484(a)(4) of the HEA (20 U.S.C. 1078-2(f) and 1091(a)(4) and 31 U.S.C. 7701(b)).

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 PII data pertaining to borrowers/co-borrowers/cosigners/students is collected and maintained by the Cornerstone[SM] System:

- Full Name
- Maiden Name
- Social Security Number
- Bank Account Numbers
- Driver's License Number and State
- Alien Registration Number
- Date of Birth
- Account Number
- Home Address
- Home Phone Number
- Mobile Phone Number
- E-mail Address
- Employment Information
- Employment Phone Number
- Medical Information (to the extent required for purposes of certain deferments and discharge requests)
- 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 status

The information is obtained from the student/borrower, co-borrowers, co-signors, references provided by the borrower, educational institutions, financial institutions, employers, the U.S. Department of Education (ED), National Student Loan Data System (NSLDS), National Student Clearinghouse, and external databases (e.g., Directory Assistance, consumer reporting agencies and skip t race vendors, U.S. Military, commercial person locator services, and U.S. Department of Treasury).

The information is collected via the following channels:

- Phone calls with customer service agents
- Entries via the interactive voice response (IVR) service
- Incoming correspondence (e.g., via U.S. mail, e-mail, etc.)
- Entry via the borrower portal web site.
- Bulk file transfers from third-party data providers
- As required, secure data transmission from ED applications, such as; NSLDS and Debt Management Collection System (DMCS), etc.
- Secure data transmission from the U.S. Department of Treasury.

The information is used to link or cross-reference multiple internal databases.

Web Databases – Borrowers can apply on-line for deferments and forbearances. The web database is used to record the on-line applications and report on web access. The web databases reside at PHEAA.

Data Warehouse (Servicing Data) - The data warehouse is used to support the Cornerstone[SM] 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.

Electronic Document Delivery – Creation of production reports for viewing, long-term retention and printing. The electronic document delivery system resides on the mainframe located at PHEAA.

Imaging – 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. The Imaging system resides at UHEAA.

Interactive Voice Response (IVR) – The IVR table houses information for use by the auto dialer software, containing borrower and loan information and is used to record results. The IVR system resides at UHEAA.

4. **Why is the information collected?** How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

   The information is collected to uniquely identify borrowers and to service their student loans on behalf of Federal Student Aid. It is necessary in order to track information pertinent to the borrower as well as process and service student loans throughout the loan life cycle. Collection of this information supports timely and full repayment of federal student loans and enables UHEAA 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.

   The privacy risks identified are unauthorized access and unauthorized disclosure of borrower PII. These risks are mitigated through technical, operational and management security controls. Access to PII is limited to only those employees and contractors with a business need for such access and only that which is necessary to accomplish assigned tasks and services. Employees and contractors with access have at least a 5C clearance and employees receive security awareness training annually to enforce their responsibility to maintain the confidentiality of borrower PII. All system users are uniquely identified and access is authenticated using strong passwords. Access into the network is restricted with firewalls; and intrusion prevention systems and malicious code protection are deployed to alert and prevent attacks. Transmission of PII across public networks is encrypted and PII stored on portable media is encrypted or otherwise physically protected. Network, server and telecommunications equipment and media are physically protected and the facilities are monitored for unauthorized access. The security controls are tested through software vulnerability scanning, annual security assessments and a formal authorization process. An incident response capability is in place to respond to security breaches and facilitate a timely containment, eradication and recovery from security incidents. Additional information regarding risk mitigation and security safeguards is provided in Section 11.

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.

Collection of applicant/borrower SSN is required for participation in Federal Student Loan programs. The SSN is the unique identifier for Title IV programs and its use is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under Federal laws and regulations. Trading partners include the Department of Education, Internal Revenue Service, and institutions of higher education, nationwide consumer reporting agencies, lenders, and servicers.

The Cornerstone[SM] System uses the SSN for the following functions:

- To verify identity and determine eligibility to receive a benefit on a loan (such as deferment, forbearance, discharge or forgiveness) under the Title IV loan programs.
- As a unique identifier in connection with the exchange of information between the Cornerstone[SM] System and its trading partners (e.g. educational institutions, financial institutions, loan services, and consumer reporting agencies) that is performed in association with the servicing of the loans.
- As a data component for submission of loan data to the U.S. Department of Education, NSLDS and Tax Form 1098E or 1099C data to the Internal Revenue Service (IRS).
- To locate the borrower and to report and collect on the loans in case of delinquency or default.

A unique account number is assigned to each borrower which is used to communicate with the borrower in lieu of the SSN. The borrower has the option to use the account number in place of the SSN during identification processes and interaction with the Cornerstone[SM] System. In the event the borrower chooses to use the SSN, the Cornerstone[SM] System uses the SSN for the following functions:

- To verify borrower identity when establishing an online account with the Cornerstone[SM] System. Once the account is created, the borrower receives a user ID and password, which are used for future authentication when using the Cornerstone[SM] System borrower portal.
- To identify borrowers who call into the IVR or customer service call center.

The account number is not an accepted identifier with trading partners or third-party data platforms that interface with the Cornerstone[SM] System.

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 in performance of Federal Student Aid business related to student loans and is necessary to adequately service and ensure successful collection of loans.

   The Cornerstone[SM] System uses the information to support the following capabilities:

   - Support for its 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, claims, and correspondence history files.

- Account management and customer access for borrowers. The Cornerstone[SM] System currently provides a secure web site 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 Cornerstone[SM] System.
- External uses of the information include:

    - Reporting to consumer reporting agencies for purposes of credit reporting.
    - Reporting to Directory Assistance to verify phone numbers.
    - Educational institutions for educational data and address verification.
    - US Postal database to check the validity of zip codes entered and to validate address updates.
    - State's department of motor vehicles for borrower's address verification to support skip-tracing activities.
    - Skip trace vendors to verify/obtain updated borrower contact information.
    - Bankruptcy notification vendors to verify/obtain updated borrower bankruptcy case information.
    - Tax assessor offices to verify/obtain updated borrower contact information.
    - Provide information to NSLDS, which is used by educational institutions for purpose of determining eligibility for programs and benefits.
    - Person locator services 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 UHEAA and PHEAA employees. Specific methods used include manual calculations and analysis of data using desktop query tools and Statistical Analysis System (SAS), which, are run both against the production environment and in the data warehouse, as well as regularly scheduled automated processes.

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?

   The Internal U.S. Department of Education organizations with which the information will be shared are 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
   - eCampus Based, future
   - 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 and 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?

The information will be shared with the following non-Department of Education organizations, 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, Intra-Governmental Payment and Collection System (IPAC), and, Ca$hLinkII)
- United States Postal Service
- Educational institutions
- Direct loan servicers and other servicers
- Independent auditors
- National consumer reporting agencies
- Person locator services
- Bankruptcy notification services
- Mail service organizations
- Other parties as authorized by the borrower

All information described in Section 3 may be shared. The information is not shared with any external entities, except to process and service the borrower's loans and as permitted by the Privacy Act of 1974 (5 U.S.C. 552a). The information is only shared as required to complete Federal Student Aid business related to the student loans. Information shared outside of the Department of Education is shared through secure encrypted transmissions, secure e-mail, and encrypted or otherwise physically secured portable media.

Sharing of information with Federal government agencies will be pursuant to an Memorandum of Understanding (MOU) or Interconnection Security Agreement (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.

See response to Section 4 to review the risk to privacy from external sharing and disclosure and how the risks are mitigated. Additionally:

All data is encrypted or otherwise secured, as appropriate, as it moves between the Cornerstone^{SM} System and the Department of Education systems, government systems, schools, guaranty agencies, lenders, servicers, independent auditors, private collection agencies, national consumer reporting agencies, the United States Postal Service, person locator services, and mail service organizations.

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, a privacy notice is sent to the borrower by letter or e-mail upon initial conversion to the Cornerstone[SM] System and on an annual basis thereafter for the life of the loan.
- A privacy policy is posted on the Cornerstone[SM] System secure borrower portal web site at https://myaccount.mycornerstoneloan.org.
- In order to establish an online account on the Cornerstone[SM] System secure borrower portal web site, the borrower must agree to the terms of service, which incorporates the privacy policy by reference and link.

The borrower has the opportunity to decline to provide information to the Cornerstone[SM] System; however, providing certain information is required in order to (i) communicate with the Cornerstone[SM] System through its secure borrower portal web site or the customer service call center, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness). The Cornerstone[SM] System does not use the information except to process and service the borrower's loans and as permitted by the Privacy Act of 1974 (5 U.S.C. 552a).

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

http://www.uheaa.org/aboutUs03.html
http://www.mycornerstoneloan.org
http://mycornerstoneloan.org
https://myaccount.mycornerstoneloan.org
http://www.mycornerstoneloan.com
http://mycornerstoneloan.com
http://www.mycornerstoneonline.org
http://mycornerstoneonline.org
http://www.mycornerstoneonline.com
http://mycornerstoneonline.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 C&A been completed? Is the system compliant with any federal security requirements?

PII is protected 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.

Access Control:
A formal, documented Access Control Policy, that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance, along with formal, documented procedures to facilitate the implementation of the Access Control Policy and associated access controls, is disseminated and periodically reviewed and updated when necessary.

Proper identification is required to establish system access and access is granted based on a valid access authorization and intended system usage. All users are assigned a unique identifier. Guest/anonymous accounts are specifically authorized and the use of such accounts is monitored. All unnecessary accounts are removed, disabled or otherwise secured. Inactive user accounts are disabled automatically. The concept of least privilege is employed, allowing only authorized access and

privileges for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with agency missions and business functions.
System access is authenticated with strong passwords and remote access requires 2-factor authentication.

Audit and Accountability:
Event logs from authentication sources, network devices, and security technologies are centrally captured and contain sufficient information to establish the type of event, the date and time the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. The event logs are secured from unauthorized viewing, modification and deletion.

System and Communication Protection:
Boundary protection measures are employed to safeguard the Cornerstone[SM] System and control information flow between information systems. All Internet traffic originating from within the Cornerstone[SM] System is controlled through proxies and content filters. Firewalls are deployed at the Internet boundary and between differing internal security zones to control traffic into and out of the Cornerstone[SM] System. The internal network is segmented based on security levels, e.g. user workstations, servers, database servers, and Internet accessible servers (DMZ).

The confidentiality and integrity of information transmitted between the Cornerstone[SM] System and other external systems is protected by cryptographic mechanisms. All inbound and outbound Cornerstone[SM] System traffic is inspected using an industry standard intrusion protection system. All portable media, such as paper, backup tapes, and CDs, are encrypted or otherwise physically secured and accountability for the portable media during transport is maintained.

Cornerstone[SM] System servers and workstations have malicious code protection installed and operational. Incoming electronic mail is scanned for spam and viruses and cleansed or quarantined when necessary.

Personnel Security:
Employees receive annual security awareness training and are specifically instructed on their responsibility to protect the confidentiality of borrower PII.

All Cornerstone[SM] System users with access to PII are required to submit to a security background check and to obtain at least a 5C security clearance.

Physical Security:
Physical access to the facility is controlled through the use of proximity readers and individually assigned keycards. Employees wear identification badges. All visitors who access non-public areas must provide photo identification and their access is recorded. Visitors are given visitor IDs and are escorted at all times. The physical security of the facility is monitored 24 hours a day, 7 days a week by security personnel. Video images from cameras are captured and digitally recorded.

Certification and Accreditation (C&A) has not been completed for the Cornerstone[SM] System.
We anticipate the Certification and Accreditation (C&A) will be completed in January 2012. A C&A has been completed on the major system components hosted by PHEAA resulting in an Authority to Operate from FSA.

The Cornerstone[SM] System is compliant with the following Federal Standards and Guidelines

- Federal Information Control 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 Information Technology 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, 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 800-44 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, September 2002
- NIST SP 800-50 Building an Information Technology Security Awareness Program, 2nd Draft, October 2003
- NIST SP 800-53 Revision 3 Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-55 Rev 1 Security Performance Metrics Guide for Information Technology Systems, 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 Appendixes 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 Information Systems Development Lifecycle, October 2008
- NIST 800-65 Integrating IT Security into the Capital Planning and Investment Control Process
- 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 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 PII, April 2008
- 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

- Department of Education Information Assurance Security Policy
- Department of Education Information Technology Security Certification and Accreditation Procedures
- Department of Education General Support System and Major Application Inventory Procedures
- Department of Education Information Technology Security Configuration Management Planning Procedures
- Department of Education Information Security Incident Response and Reporting Procedures
- Department of Education Protection of Sensitive But Unclassified Information
- Department of Education Personal Use of Government Equipment
- Department of Education Lifecycle Management (LCM) Framework
- Department of Education Procuring Electronic and Information Technology (EIT) in Conformance with Section 508 of the Rehabilitation Act of 1973
- Department of Education Contractor Employee Personnel Security Screenings
- Department of Education IT Security Awareness Training
- Department of Education Privacy Safeguards Training

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?

    The Cornerstone[SM] System will be covered under the System of Records Notice entitled 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:

    Cornerstone[SM] System uses the Department of Education records retention and disposition schedule. Records will be covered under the following schedule: ED 75/N1-441-09-16: Federal Student Aid Loan Servicing, Consolidation, and Collections Records