



## **Privacy Impact Assessment**

### **For:**

Not-For-Profit New Mexico (NFP New Mexico)  
Pillar Fed Servicing System

### **Date:**

November 30, 2012

### **Point of Contact:**

Calvin Whitaker  
202-377-3045  
[Calvin.Whitaker@ed.gov](mailto:Calvin.Whitaker@ed.gov)

### **System Owner:**

Keith Wilson  
202-377-3591  
[Keith.Wilson@ed.gov](mailto:Keith.Wilson@ed.gov)

### **Author:**

Carolyn Holder  
505-761-2360  
[holder@nmstudentloans.org](mailto:holder@nmstudentloans.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.**

<b>Information System Name</b>	<b>System Acronym</b>	<b>Operator of the System (on behalf of Federal Student Aid)</b>
Pillar Fed Servicing/Not-for-Profit New Mexico	NFP New Mexico	PHEAA

The Pillar Fed Servicing/Not-for-Profit New Mexico system (NFP New Mexico) operated by the Pennsylvania Higher Education Assistance Agency (PHEAA) is hereafter referred to as Not-For-Profit New Mexico (NFP New Mexico). Operational capabilities of the system include borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, borrower correspondence; call scheduling, collection, skip-tracing and correspondence history files.

The NFP New Mexico 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.

NFP New Mexico subcontracts with PHEAA to manage the NFP New Mexico system. PHEAA is responsible for the maintenance and operations of the NFP New Mexico system.

**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, 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 NFP New Mexico system collects and maintains the following PII data pertaining to borrowers/co-borrowers/co-signers/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
- Home, work, alternate and mobile telephone number
- Financial information
- Email address
- Employment information
- Related demographic data
- 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 the student/borrower, co-borrowers, co-signers, references provided by the borrower, educational institutions, financial institutions, employers, U.S. Department of Education (DoED), the National Student Loan Data System (NSLDS), National Student Clearinghouse (NSC) and external database (e.g., Directory Assistance, consumer reporting agencies, skip-trace vendors, U.S. Military, commercial person locator services and U.S. Department of the 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, email, etc.)
- Entry via the Borrower Portal Web site Refer to question 10 hereof.
- Bulk file transfer from third-party data providers as required, secure data transmission from DoED applications, such as: NSLDS and Debt Management Collection System (DMCS), etc.
- Secure data transmission from the U.S. Department of the Treasury.

The information is used in connection with loan processing and servicing activities, such as identity verification and authentication during online account creation and telephone calls, verification between internal databases within the NFP New Mexico system and data exchange with external trading partner databases such as:

- Consumer reporting agencies
- Lending institutions and other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system
- Educational institutions.

- 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 necessary to uniquely identify borrowers and to service their student loans on behalf of Federal Student Aid. The NFP New Mexico 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 NFP New Mexico to assist borrowers with managing their loans. The information is also needed to determine borrower eligibility for entitlements such as deferments, forbearances, discharges and to locate borrowers in cases of invalid addresses and/or telephone numbers. The servicing of student loan functions entails the following:

- Verifying loan detail
- Mailing of forms for loan forbearance, deferment and repayment option modifications
- Mailing/emailing of statements of account
- Mailing of change of address inquiries
- Verifying identity for account management
- Identifying and verifying borrowers during loan conversion/de-conversion
- Scheduling due diligence calls
- Issuing loan discharge and forgiveness claims and correspondence
- Maintaining and preparing loan and account history records and reports
- Planning for audit and program review
- Optimizing internal processes
- Providing information to track refunds/cancellations
- Transmitting loan information to FSA loans central processing platform via DoED applications such as NSLDS, DMCS and Total and Permanent Disability System (TPD).

Privacy risks would result from a breach of NFP New Mexico's and PHEAA's security safeguards as implemented on the NFP New Mexico system, which could compromise the confidentiality, integrity and availability of information. The most likely method of breach would be through unauthorized access that would enable an adversary to disclose, damage the integrity of, or prevent the availability of information. Another type of risk would be a man-made or natural disaster destroying the data center or place of business.

Key Risk Mitigation Measures include:

- 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/firewall log monitoring, malware detection and removal software, Virtual Private Networks (VPN) and encryption at the perimeter
- All external electronic transmissions used to receive or send PII data are encrypted
- To protect unauthorized access to NFP New Mexico and PHEAA employees, audit logs are maintained and reviewed at regular intervals and NFP New Mexico system access is restricted by limiting the access based on the principle of least privilege



- Unauthorized system use by NFP New Mexico and PHEAA employees is subject to strict penalties
- All NFP New Mexico and PHEAA personnel are required to obtain government security clearance, to read and acknowledge the Rules of Behavior and to complete an initial security training and awareness course as well as periodic refresher training
- All NFP New Mexico and PHEAA infrastructure is located in facilities that leverage appropriate environmental controls
- NFP New Mexico and PHEAA maintain appropriate systems for redundancy and failover
- Borrower accounts accessed via the IVR or customer service call centers require appropriate authentication
- Borrower accounts accessed via the secure website require multi-factor authentication
- NFP New Mexico and PHEAA maintain incident response, disaster recovery and business recovery plans to minimize impact of any failures/outages from man-made or natural disasters
- NFP New Mexico and PHEAA require annual security training for all employees and implement security controls as mandated by the Federal Information Security Management Act (FISMA). 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.

**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 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 law and regulations. Trading partners include the Department of Education, Internal Revenue Service (IRS), institutions of higher education, national credit bureaus, lenders and servicers.

The NFP New Mexico 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)
- As a unique identifier in connection with the exchange of information between the NFP New Mexico 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 DoED NSLDS and Tax Form 1098-E data to the IRS
- To locate the borrower and to report and collect on the loans in case of delinquency or default.



NFP New Mexico assigns a unique account number to each borrower that is used to communicate with the borrower in lieu of the SSN. The borrower has the option to use NFP New Mexico's system account number in place of the SSN during the identification process when communicating with NFP New Mexico and interacting within the NFP New Mexico system. In the event the borrower chooses to use the SSN, the NFP New Mexico system uses the SSN for the following functions:

- To verify borrower identity when establishing an online account with the NFP New Mexico system. Once the account is created, the borrower receives a User ID and password, which are used for future authentication when using the NFP New Mexico system borrower portal
- To identify borrowers who call into the IVR or customer service call center.

This unique account number is not an accepted identifier with trading partners or third-party data platforms that interface with the NFP New Mexico system; the SSN is required for these types of transactions.

**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 NFP New Mexico to perform Federal Student Aid business related to student loans and is necessary to adequately service and ensure successful collection of loans.

The NFP New Mexico system will employ 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
- Provide three major forms of account management and customer access for borrowers. The NFP New Mexico 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 NFP New Mexico 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
- 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 NFP New Mexico and PHEAA employees. Specific methods used include manual calculations and analysis of data using desktop query tools and SAS (Statistical Analysis System).

**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 NFP New Mexico 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. NFP New Mexico 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 question 4, which describes what information is shared, for what purpose the information is shared, 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?**

All information described in question 3 hereof may be shared.

NFP New Mexico 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 Applications vendor, Pay.gov, Remittance Express, Integrated Professional Automation Computer and Ca\$hLinkII)



- United States Postal Service (to obtain updated contact information).

NFP New Mexico 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 NFP New Mexico 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 NFP New Mexico system in connection with NFP New Mexico servicing of DoED loans).

NFP New Mexico does not share the information with any external entities except to process and service the borrower's loans and as permitted by the Privacy Act of 1974. 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 and email.

Sharing of information with Federal government agencies will be pursuant to a 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 question 4 hereof to review the risk to privacy from external sharing and disclosure and how the risks are mitigated.

Additionally:

- All information is protected by multi-factor authentication and monitored by automated and manual controls
- Data is housed within PHEAA's sub-contractors' secure data center facilities
- All data is encrypted or otherwise secured, as appropriate, as it moves between the NFP New Mexico system and DoED 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, NCOA and any approved entity.



**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](http://www.fafsa.ed.gov))
- A privacy policy is also posted on NFP New Mexico's secure borrower portal website
- In order to establish an online account on the NFP New Mexico system secure borrower portal website, the borrower must agree to the Terms of Service, which incorporates the privacy policy by reference and link.

NFP New Mexico will send a written Privacy Notice to borrowers, which is included in their Welcome Package, when they initially convert to the NFP New Mexico system and annually thereafter.

In order to establish an online account on the NFP New Mexico secure borrower 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 NFP New Mexico; however, providing certain information is required in order to (i) communicate with the NFP New Mexico through its secure borrower Web site or the NFP New Mexico's customer service call center, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness).

NFP New Mexico does not use the information except to process and service the borrower's ED loans and as permitted by the Privacy Act of 1974.

We reserve the right to change our Online Consumer Information Privacy Policy. Any changes to our Online Consumer Information Privacy Policy will be reflected in the updated version displayed at our corresponding website.

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

[www.fafsa.ed.gov](http://www.fafsa.ed.gov)

[www.nmeaf.org](http://www.nmeaf.org)

[www.nmstudentloans.com](http://www.nmstudentloans.com)

[www.mypillarloan.com](http://www.mypillarloan.com)

[www.mypillar.org](http://www.mypillar.org)

[www.pillarfedservicing.com](http://www.pillarfedservicing.com)

[www.pillarfedserciving.org](http://www.pillarfedserciving.org)



**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?**

In accordance with the Federal Information Security Management Act of 2002 (FISMA), every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. The NFP New Mexico is scheduled to receive its ATO on May 15, 2013.

FISMA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Additionally, the following specific controls are applied:

Management Controls

- Certification, Accreditation and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational Controls

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environment Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical Controls

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)



NFP New Mexico employs administrative, technical and physical security controls of its facilities and systems in accordance with FISMA.

#### 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. 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 processing 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 multi-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 types 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 NFP New Mexico system and control information flow between information systems. All Internet traffic originating from within the NFP New Mexico system is controlled through proxies and content filters. Firewalls are deployed at the Internet boundary.

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

The NFP New Mexico system servers and workstations have malicious code protection installed and operational. Incoming electronic mail is scanned for spam and viruses and is 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 PII. All NFP New Mexico systems 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 cards. Employees wear identification badges. All visitors who access non-public areas must provide photo identification, and each person's access is recorded. Visitors requiring an escort are given red "escort required" badges which must be worn at all times in the facility. The physical security of the facility is monitored 24 hours a day, 7 days a week by a monitoring company. Video surveillance from cameras is captured and digitally recorded 24/7.

Security Authorization (SA) The Security Authorization has not been completed for the NFP New Mexico system. We anticipate the SA process to be completed on May 15, 2013.

The NFP New Mexico system is compliant with the following Federal Standards and Guidelines:

- Federal Information Security Management Act (FISMA)
- Privacy Act of 1974
- E-Government Act of 2002
- 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?**

NFP New Mexico 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, NFP New Mexico will follow the FSA “Loan Servicing, Consolidation and Collections Records” records schedule. 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 Consolidation System (DLCS)  
Total and Permanent Disability (TPD)  
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