



Privacy Impact Assessment

For

**Not-For-Profit Iowa Student Loan (NFPISL)
Aspire Resources, Inc. (Aspire) Information System**

Date:

March 9, 2015

Point of Contact:

Andre E. Nicholas
andre.nicholas@ed.gov

System Owner:

Keith Wilson
keith.wilson@ed.gov

Author:

Tim Pegg
tpegg@studentloan.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. Indicate whether the system is new or existing and whether or not the PIA is new or being updated from a previous version; specify whether the system is “agency” or “contractor.”

Information System Name	System Acronym	Operator of the System (on behalf of Federal Student Aid)
Not-For-Profit Iowa Student Loan	NFPISL	Aspire Resources, Inc., Iowa Student Loan, PHEAA

The Not-For-Profit Iowa Student Loan System (NFPISL) is an existing system operated by Aspire Resources, Inc. and Iowa Student Loan in concert with the Pennsylvania Higher Education Assistance Authority (PHEAA). This PIA has been updated from a previously existing version.

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 NFPISL system communicates with the internal Federal Student Aid (FSA) platforms, borrowers, other loan servicers, third-party data providers, consumer reporting agencies, guarantors and government agencies (as permitted by the Federal Privacy Act of 1974). Channels of communication include U.S. mail, telephone calls, a secure borrower website, secure email and secure data transfer links.

2. Legal Authority.

Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The Higher Education Act of 1965 (Public Law 89–329), as amended, sections 428, 484, and 485B; 31 U.S.C. 7701; and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

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 NFPISL 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

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 databases (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, verification between internal databases within the NFPSL 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.

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

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

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

5. Social Security Number (SSN).

If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

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

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

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



6. Uses of the Information.

What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

This information is collected to meet the contractual requirements of Federal Student Aid, enabling NFPISL to perform student loan servicing activities.

The information is used for identification and verification purposes. Information is also used to assist borrowers with managing their loans, determine borrower eligibility for entitlements such as deferments, forbearances, and discharges, and to locate borrowers in cases of invalid addresses and/or phone numbers.

The information is used by trading partners for the purposes of default management, program eligibility, credit history, person locator services and general account maintenance.

The data is analyzed and evaluated for the purposes of maintaining account balances, debt collection, default prevention, repayment assistance forms, and general account maintenance.

Sources of information will be various Federal agency databases, servicers from whom the Department of Education purchases student loans, person locator services and consumer reporting agencies.

7. Internal Sharing and Disclosure.

With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

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

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

All or part of the information described in Question 3 may be shared.

The information is only shared as required by FSA.

See response to Question 4 for risks and mitigation measures.



8. External Sharing and Disclosure.

With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

NFPISL is 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, Pay.gov, Credit Gateway, Intra-Governmental Payment and Collection System and Collections Information Repository)
- United States Postal Service (to obtain updated contact information).
- Department of Defense

Information will be shared with the following non-governmental entities:

- Educational Institutions
- Other Federal Loan Servicers
- Independent Auditors
- National Consumer Reporting Agencies
- Person Locator Services
- Other parties as authorized by the borrower

All or part of the information described in Question 3 hereof may be shared.

The information is only shared as required by Federal Student Aid.

Information is shared through file and secure email transmissions using encryption methods compliant with Federal requirements.

Sharing of information with nongovernmental entities (consumer reporting agencies, independent program participants, etc.) will be pursuant to contractual or regulatory requirements, or through sharing agreements between the applicable entities and the Department of Education.

See response to Question 4 for risks and mitigation measures.

9. Notice.

Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A privacy notice/policy is presented to the borrower via the following channels:

- Pursuant to the Gramm-Leach-Bliley Act, DoED’s privacy notice is sent to the borrower by letter or email upon purchase of the loan by DoED and on an annual basis thereafter for the life of the loan



- A privacy notice is provided on the Free Application for Federal Student Aid (FAFSA) form and on the FAFSA online application website (www.fafsa.ed.gov)
- A privacy policy is also posted on NFPISL's secure borrower portal website (www.aspireresourcesinc.com)
- In order to establish an online account on the NFPISL system secure borrower portal website, the borrower must agree to the Terms of Service, which incorporates the privacy policy by reference and link.

Borrowers can at this point decline to provide additional information; however, providing certain information is required in order to communicate with Aspire through its secure borrower Web site and/or customer service call center.

Borrowers are required to opt into online account access features, and are required to provide consent, in compliance with applicable law, for various features and services provided by the NFPISL system, such as paperless document delivery and online payment services.

NFPISL shares information with designated financial, education, and Department of Education organizations and contractors only as required by contract..

10. Web Addresses.

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

www.aspireresourcesinc.com/Contact-Us/Privacy/privacy-policy.aspx

www.aspireresourcesinc.com/Contact-us/Privacy/Online-Privacy-Statement.aspx

www.fafsa.ed.gov

11. Security.

What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

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 NFPISL system received its ATO on March 29, 2012.

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)

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

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 1978.

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 NFPISL system and control information flow between information systems. All Internet traffic originating from within the NFPISL system is controlled through proxies and content filters. Firewalls are deployed at the Internet boundary.

The confidentiality and integrity of information transmitted between the NFPISL system and other external systems is protected by cryptographic mechanisms. Inbound and outbound NFPISL 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.

The NFPISL system servers and workstations have malicious code protection installed and operational. Incoming electronic mail is scanned for spam and viruses and is cleaned 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 NFPISL 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.

Certification and Accreditation (C&A)

The Certification and Accreditation has been completed for the NFPISL system. The C&A process were completed on March 29, 2012. A C&A has been completed on the major system components hosted by PHEAA resulting in their receiving an Authority to Operate (ATO) from FSA.

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

- Federal Information Security Management Act (FISMA)
- Privacy Act of 1974, as amended
- 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 General Support System and Major Application Inventory Procedures
- Department of Education Handbook for Information Technology Security
- 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?

NFPISL 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, NFPISL will follow the FSA Loan Servicing, Consolidation, and Collections Records. The ACS Tracking Number is OM: 6-106:L74.

DoED Record Schedule:

Schedule Locator NO: 075

Draft Date: 03/11/2009

Title: FSA Loan Servicing, Consolidation and Collections Records

Principal Office: Federal Student Aid

NARA Disposition Authority: N1-441-09-16

Description:

These records document business operations that support the servicing, consolidation, and collection of Title IV federal student aid obligations. These records relate to the post-enrollment period of student aid, including servicing of direct loans, consolidation of direct loans, managing and recovering defaulted debts



assigned to the Department from Federal Family Education Loan (FFEL) and other lenders, rehabilitated loans, and any other type of Title IV student aid obligation.

This schedule provides a common disposition for records that comprise a variety of material and media, including but not limited to demographic and financial data on individual borrowers; institutional data on schools, guarantors, lenders, private collection agencies; records of financial transactions, payments, collections, account balancing and reconciliation, and reporting; records pertaining to customer interactions; and related correspondence and documents.

As these records may be maintained in different media formats, this schedule is written to authorize the disposition of the records in any media (media neutral). Records that are designated for permanent retention and are created and maintained electronically will be transferred to NARA in an approved electronic format.

DISPOSITION INSTRUCTIONS:

a. Record Copy

TEMPORARY

- Cut off annually upon payment or discharge of loan. Destroy/delete 15 years after cut off.

b. Duplicate Copies Regardless of Medium Maintained for Reference Purposes and That Do Not Serve as the Record Copy

TEMPORARY

- Destroy/delete when no longer needed for reference.

ELECTRONIC INFORMATION SYSTEMS:

Direct Loan Consolidation System (DLCS)

Total and Permanent Disability (TPD)

Debt Management and Collection System (DMCS)

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.

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.