Privacy Impact Assessment

For:

Aspire Resources Inc. Federally Owned Debt Information System (NFP-ARI)

Date:

October 28, 2011

Point of Contact:
Jamette Bell
(202) 377-3388
jamette.bell@ed.gov

System Owner:
Cindy Bartz
(515) 273-7114
cbartz@studentloan.org

Author:
Tim Pegg
(515) 273-7846
tpegg@studentloan.org

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.**

   Aspire Resources Inc.SM (Aspire) is located in West Des Moines, Iowa. The Aspire Resources Inc. Federally Owned Debt Information System (NFP-ARI) is a secure system that supports the management and servicing of Department of Education Office of Federal Student Aid (FSA) Title IV student loans. The NFP-ARI information system provides a complete servicing solution that includes: on-site call center; on-site fulfillment printing; loan processing, which includes but is not limited to, deferment and forbearance processing; collection and skip-tracing capability; integrated electronic document management; and financial reporting and reconciliation services. The NFP-ARI information system consists of a tiered defense-in-depth secure network environment with redundancy at multiple levels to ensure high availability. All of Aspire accomplishes its entire loan servicing activities and data processing from one site.

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 following provide legal authority for Aspire to collect and use the associated data:

   - Titles II, IV–A, IV–B, IV–D, IV–E and V–C of the HEA (20 U.S.C. 1024, 1070a, 1070b–1070b–4, 1070c–1070c–4, 1070c–3a, 1071–1087–4, 1087a–1087j, and 1087aa–1087ii, and 1104 (1998); 31 U.S.C. Chapter 37).
   - Higher Education Act of 1965 as amended §428 and §484(b)(4) and Code of Federal Regulations: 34 CFR §668 and §682

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-ARI System shall contain records on individuals (borrowers, co-borrowers and references) that Aspire collects and maintains for the U.S. Department of Education.

   Information gathered on individuals includes the following:
   - Full name (first name, last name and middle initial)
   - Social Security number
   - Date of birth
   - Address
   - Telephone numbers (home, work and alternate)
   - Email address
   - Employment information
   - Loan information

   Loan information includes the following:
   - Disbursement amount
   - Principal balance
   - Interest accrual
   - Repayment plan
   - Repayment amount
   - Payment history

- Loan status (forbearance, deferment, etc.)
- Separation date
- Grace period
- Bank account information
- Delinquency

The sources for this data shall include borrowers, co-borrowers, employers, educational and lending institutions, and other sources (e.g., the National Student Loan Data system [NSLDS], TransUnion, etc).

The information shall be collected via paper form, website, electronic data transmission and telephone.

This information shall be used to cross-reference multiple databases to service the loan.

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.**

Information collected by NFP-ARI shall be collected to support Federal Loan Servicing in accordance with Aspire's contractual obligations with the U.S. Department of Education office of Federal Student Aid (FSA). The information shall be used for loan detail correspondence, notifications, and corrections. It shall provide for identity assurance during communications with borrowers during the course of account maintenance. Information collected will be used to support loan conversion activities, account audits, and enhance the accuracy of information described within the account.

Primary risks to privacy of the data are described in terms of confidentiality and integrity. Risks to confidentiality and integrity come from the following threat sources: authorized human intentional, authorized human unintentional, unauthorized human intentional and technological.

Mitigation of authorized human intentional threat vectors is through the use of background screening, appropriate education and departmental policy. Additionally account access is limited based on least privilege and a valid business mission. Separation of duties supports the mitigation of authorized human intentional compromise of confidentiality.

Corporate policy and security training reduce the threat of authorized human unintentional threat vectors to information integrity. Periodic backups mitigate additional risks to information integrity and also provide for its availability.

Mitigation from unauthorized human intentional threats to integrity and confidentiality are provided by account management, automated logging and alerting, incident response plans and formalized secure communication procedures. Physical security ensures that only authorized personnel are allowed physical access to the computing environment and system integrity applications provide assurances to the security of supported systems.

Risks from the threats of technological sources are reduced by the same controls as unauthorized human intentional threats. Additionally anti-virus, Web filtering, patch management along with periodic vulnerability assessments ensure a low residual risk to the information from technological threats.

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 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.

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 within NFP-ARI will be used to provide customer service, loan processing and loan-collection support related to servicing of federally owned Title IV student loan debt. This includes, without limitation, performing loan conversion activities, processing consolidation payoffs, answering inquiries, performing document imaging and retention, performing fulfillment and mail processing, processing accounts, collecting delinquent debt, processing payments, performing reconciliation, providing NSLDS support and completing Total and Permanent Disability (TPD)/ Data Management Collection System (DMCS) processing.

Standard methods of account reviews are used to analyze loan activities to support loan servicing.

Publicly and commercially available information is used to provide different avenues to contact people to service their loans and to ensure the accuracy of the information maintained in the 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?**

DoED entities:
- Financial Management System (FMS)
- National Student Loan Data System (NSLDS)
- Debt Management Collection System (DMCS)
- Total and Permanent Disability (TPD)
- Post Secondary Education Participant System (PEPS)
- Common Origination and Disbursement System (COD) - (including eMPN and TEACH ATS)
- Student Aid Internet Gateway (SAIG)
- Common Services for Borrowers (CSB) DataMart or future datamarts, optional
- eCampus Based, future

Any information that is listed in section 3 may be shared.

The information shall only be shared to fulfill contractual obligations with FSA.

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?

Non-U.S. Department of Education interfaces include, but are not limited to:
- Schools
- Guaranty agencies
- Lenders, lender servicers, Direct Loan Servicer, and other servicers
- Independent auditors
- Private collection agencies (PCAs)
- National consumer reporting agencies
- United States Postal Service (USPS)
- Skip tracing vendors
- E-Oscar - credit reporting dispute interface

Any information that is listed in section 3 may be shared.

The information is shared to fulfill contractual obligations with FSA and business related to servicing student loans.

Information is shared outside of the U.S. Department of Education using secure electronic communication. External electronic transmissions of PII are encrypted.

Memorandum of Understandings or Inter System Agreements shall be established in accordance with FSA guidance and/or in compliance with other contractual or regulatory requirements.

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?**

Aspire will provide disclosure notices to borrowers as required by FSA, laws, regulations and contractual obligations. Aspire shall provide opportunities to individuals to decline to provide information and have individual grant consent in accordance with FSA requirements.

10. **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?**

Administrative safeguards:
- Automated account management and control is documented and reviewed.
- There are managerial account reviews occurring periodically.
- Policy is reviewed to ensure that technical controls are supported.
- Tiered security awareness training educates users to support security policies.
- Acceptable use policy and rules of behavior support user education.
- System use notifications warn and advise users of the system on system expectations.
- Configuration management change control ensures changes in Aspire's environment are reviewed and communicated.
- System hardware and software inventory controls are in place.
- Contingency plans, including alternate storage sites, are reviewed and tested.
- Accounts and authentication are consistently secured through identification and authentication policies.
- Media storage, transport and sanitization processes provide for increased data security.

Technical safeguards:

- Automatic inactive account termination has been implemented.
- Unsuccessful login attempt safeguards are enabled.
- Remote access is controlled and monitored.
- There are access controls for mobile devices.
- Centralized logging occurs with alerting and periodic review.
- Hardened secure baselines are configured on operating systems and applications.
- Information system backups are completed and recovery components are tested.
- Multifactor authentication protects privileged user's login and access.
- Boundary protected by firewalls and managed IDSs.

Physical safeguards:
- Physical access is restricted and monitored.
- Physical access is internally restricted to critical infrastructure.
- Building power is supplemented by uninterrupted power supply (UPS) and generator capabilities.
- Critical infrastructure is environmentally controlled with redundant systems.
- Facilities are monitored using video surveillance.
- A fire suppression system is implemented.
- Visitor controls and access records are maintained.

Certification and accreditation shall be accomplished with FSA during fourth quarter 2011 and first quarter 2012.

Federal Standards and Guidelines
- Federal Information Control Audit Manual (FISCAM)
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems, November 2001
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, January 2002
- NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-35 Guide to Information Technology Security Services, October 2003
- NIST SP 800-37 Information Technology Certification and Accreditation Guide, October 2003
- NIST SP 800-40 Procedures for Handling Security Patches, August 2002
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- NIST SP 800-42 Guidelines on Network Security Testing, October 2003
- NIST SP 800-44 Guidelines on Securing Public Web Servers, September 2002
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002
- NIST SP 800-50 Building an Information Technology Security Awareness Program, 2ndDraft, April 2003
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems, July 2003
- NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- NIST SP 800-60 Volume 2, Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- NIST SP 800-64 Security Considerations in the Information Systems Development Lifecycle, October 2003
- NIST Draft Special Publication 800-53, Revision 1 (Final Public Draft), October, 2006, Recommended Security Controls for Federal Information Systems

Department of Education Policies

- Department of Education Handbook for Information Technology Security 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

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

Privacy notices are planned to be online privacy policies using the following URLs:
http://www.aspireresourceinc.com/Contact-Us/Privacy-Policy-Online.aspx
http://www.aspireresourceinc.com/Contact-Us/Privacy-Policy-Customer.aspx

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-ARI 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:

N1-441-09-16 is the records schedule number related to federal servicers supplied to Aspire by FSA. Aspire shall comply with the provided schedule.