Privacy Impact Assessment

For

Financial Partners Data Mart (FPDM)

Date:
October 20, 2015

Point of Contact and Author:

Calvin Whitaker

Calvin.Whitaker@ed.gov

System Owner:

Keith Wilson

Keith.Wilson@ed.gov

Federal Student Aid (FSA)

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)**
Financial Partners Data Mart	FPDM	Virtual Data Center

The Financial Partners Data Mart (FPDM) system provides executive information and decision support capabilities around several key business functions. By collecting information from several sources into a central location, FSA and Financial Management will be able to more efficiently identify areas in which each party may assist the other while improving the support for students with the Federal Family Education Loan Program and Direct Loan Program. The FPDM provides a mechanism to generate end user reports from several ED database source systems which provides information and decision support capabilities for several key business functions:

- Portfolio Analysis: Targeting areas of fiscal risk to FSA and its financial partners (i.e., Guaranty Agencies, Lenders and Servicers). Monitoring financial partners' operating performance (risk factors) to identify and focus on areas of risk and the need for technical assistance. Reducing the time required between identifying risk areas and implementing solutions.
- Customer Relationship Management: Increasing routine, positive communication with external financial partners by providing information regarding their performance between review cycles. Assisting guaranty agencies in reviewing lenders, by providing additional information.
- Compliance Management: Focusing performance reviews to those financial partners that are not performing in accordance with standards and/or regulations. Improving the efficiency of pre-planning and analysis activities associated with the review process.
- Portfolio Management: Identifying and assessing the portfolio mix to improve policy decisions. Improving the efficiency and effectiveness of trend analysis by providing calculated benchmarks, where appropriate.

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 FPDM system collects and maintains the following PII data pertaining to defaulted borrowers:

- Full Name
- Social Security Number (SSN)
- Date of Birth
- Home Address
- Driver License Number and State
- Email Address
- Place of Birth Country
- Borrower loan information including disbursement amount, principal balance, accrued interest, loan status, repayment amount, grace period and delinquency status.

The information is obtained from the National Student Loan Data System (NSLDS) and Title IV Additional Servicers (TIVAS) system.

The information is collected via the following channels;

- Secure data/file transmission from DoED applications, such as National Student Loan Data System (NSLDS), Postsecondary Education Participants System (PEPS) and Financial Management System (FMS), Guarantee Agencies and Lenders.

The information is used in connection with loan servicing, portfolio analysis, and compliance management. These include monitoring operating performance, assisting in guarantee agencies and lender reviews, and assessing the portfolio mix using trend analysis and benchmarks.

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 required for the mission of the Agency in order to comply with the Higher Education Act (HEA) policies, regulations and *statues.*
- The information is collected is necessary for the following reasons;
- Provide default rates calculations for educational institutions, guaranty agencies, and lenders
- To perform guarantee agency and lender reviews
- To monitor compliance and analysis and to provide executive information and decision support capabilities around several key business functions
- To assess Title IV Program administration of guaranty agencies, educational institutions and servicers
- To provide default rate calculations

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 TEC employees, audit logs are maintained and reviewed at regular intervals and TEC system access is restricted by limiting the access based on the principle of least privilege
- Unauthorized system use by Technical Expert Consulting (TEC) employees is subject to strict penalties
- All TEC 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 infrastructure is located in facilities that leverage appropriate environmental controls
- TEC maintains appropriate systems for redundancy and failover
- TEC maintains incident response, disaster recovery and business recovery plans to minimize impact of any failures/outages from man-made or natural disasters

TEC requires 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, institutions of higher education, national credit bureaus, lenders, and servicers. There is no alternative to the SSN for this use. In addition, FPDM 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 FSA and its trading partners (e.g. educational institutions, financial institutions, loan services and consumer reporting agencies) that is performed in association with servicing of loans (or other appropriate language)
- As a data component for submission of loan data to DoED NSLDS and Tax Form 1098-E data to the IRS

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 used to enable FPDM to perform Federal Student Aid business related to compliance monitoring, portfolio analysis, customer management and reporting and is necessary to adequately provide executive information and decision support capabilities.

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.

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 FPDM System shares information with DoED to allow it to administer the FPDM Program. DoED may disclose information contained in a record in an individual's account in accordance with the Privacy Act of 1974. FPDM shares information with:

- Federal Student Aid and its agents or contractors
- Financial Management System (FMS)
- National Student Loan Data System (NSLDS)
- Postsecondary Education Participants System (PEPS)

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 above may be shared as stated below.

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

- Educational institutions (to coordinate the management of the loan with the educational institution's financial aid office)
- Independent auditors (SSAE16, FSA auditors)
- Freedom of Information Act (FOIA) Advice Disclosure
- Disclosure to the Department of Justice
- Contract Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosure
- Federal and State Disclosures
- Law Enforcement Disclosures
- Employee Grievance, Complaint or Conduct Disclosure
- Labor Organization Disclosure
- Congressional Member Disclosure
- 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)

FPDM 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.

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, FPDM 's privacy notice is available to the borrower via FPDM websites
- A privacy notice is provided on the Financial Partners Data Mart online website (https://fp-mart.ed.gov)

10. Web Addresses.

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

https://fp-mart.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 FPDM system received an ATO on January 16, 2014.

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)

Privacy Controls

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

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 FPDM system and control information flow between information systems. All Internet traffic originating from within the Virtual Data Center (VDC) system is controlled through proxies and content filters. Firewalls are deployed at the Internet boundary.

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

Personnel Security

Employees receive annual security awareness training and are specifically instructed on their responsibility to protect the confidentiality of PII. All FPDM 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 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 been completed for the FPDM system.

The FPDM 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. 4, Recommended Security Controls for Federal Information Systems, April 2014
- 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?

FPDM is covered under the National Student Loan Data System (NSLDS) System of Records (SORN) , which was published as Number 18-11-06 in the Federal Register on April 2, 2014 [79 FR 18534].

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:

Records are maintained and disposed of in accordance with the Department's Record Disposition Schedule ED 072, 086, 185, and 186.