Privacy Impact Assessment

For: Integrated Partner Management (IPM)

Date: March 14, 2017

Point of Contact: Adil Lahjouji

System Owner: Monica Williams

Author: Creative Ideas Simple Solutions (CISS)

Office of 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.

The Department of Education (ED) Office of Federal Student Aid (FSA) is developing the Integrated Partner Management System (IPM), which will integrate the partner management operations of FSA's business. This system will streamline, consolidate, and integrate a number of common functions within the partner management business systems to deliver significant improvements in managing partner interactions and support of the delivery of Title IV funds from both a cost and customer satisfaction perspective.

The partner management functions include enrollment, eligibility and oversight processes used to manage partner entities as they administer Title IV Financial Aid for Students. IPM is to combine and modernize FSA's partner management enterprise systems through combining the services provided by current legacy systems into a single IPM solution using Microsoft SharePoint and K2 components. This integration will take an end-to-end view of FSA's entire partner eligibility and oversight business, which includes the following legacy systems:

- Postsecondary Education Participants System (PEPS)
- Electronic Application for Approval to Participate in Federal Student Financial Aid Programs (eApp)
- eZ-Audit
- Electronic Records Management (ERM)
- Lender's Application Process (LAP)

Additionally, the routing ID (RID) data from the Common Origination and Disbursement (COD) system, as well as partner-related information, third party servicers (TPS) data will be migrated to IPM from COD. COD will transfer the responsibility to generate new RIDs to IPM when it goes live. Destination Point Administrator (DPA) data will be migrated to the IPM database from Participation Management (PM).

The IPM System endeavors to provide the following benefits:

- Improve efficiency of staff by implementing workflow automation to ensure timely completion and accountability for the Partner eligibility and enrollment process
- Improve efficiency of staff by for Case Management and a seamless repository for information access and retention
- Provide a scalable and configurable platform to provide the maximum flexibility in meeting FSA and Partner needs today and well into the future
- Reduce FSA risk by leveraging current technologies and products used at FSA to replace out of date and unsupported technologies
- Establish a base of secure and accessible information

- Provide efficient processes that meet internal and external reporting requirements
- Improve the overall quality of program compliance by reducing errors, conducting more complete analysis and receiving timely results
- Assure flexibility in structuring and staffing the program compliance function
- Reduce the risk of FSA failing to detect a non-compliant partner.

The short description of each legacy system is provided below:

Postsecondary Education Participants System (PEPS). PEPS is a repository containing all information related to Title IV student aid delivery. PEPS stores information for schools, lenders, guaranty agencies (GAs), demographic information for partners, current and historical eligibility information, financial, compliance audit and oversight related data. PEPS provides information to a large number of agencies, including partners, State Licensing and Accrediting Agencies, lenders, servicers, Federal and State Governments as well as general public. PEPS data will be the largest legacy data source migrated to the IPM data repository

Electronic Application for Approval to Participate in Federal Student Financial Aid Programs (eApp). eApp is a web-based application for approval to participate in Title IV programs. APP provides postsecondary institutions with the functionality to designate the eligibility and apply for initial participation, recertification, reinstatement, change in ownership, and the ability to update a current approval. eApp has its own data repository, but all eApp tables are replicated in PEPS database.

eZ-Audit. This system provides an automated workflow process and web-based access interface for submitting financial statements and compliance audits to schools participating in Title IV programs. By retaining PDF files as the official record and a means to validate data, eZ-Audit allows the Federal Student Aid to check the accuracy of a school's submission, correct electronic data, and provide a central repository and historical archive for all related documents. eZ-Audit also provides information and notifications related to the status of application submissions for schools.

Integrated Partner Management Document Management (IPM DM) System is an interim solution, which was developed and released early to support the Department of Education's Federal Student Aid (FSA) Office in converting paper documents into an electronic format. The primary objective of IPM DM was to replace FSA's legacy Electronic Records Management (ERM) system and to improve the efficiency of FSA's document management process within the Program Compliance Office. The IPM DM system maintains approximately one million documents in the system. The major categories of documents are Audit, Eligibility & Certification, Financial Analysis, Method of Payment, and Program Review. The IPM DM

system provides litigation support for management decision, show compliance with Government regulation, and supply historical information.

Lender's Application Process (LAP). The LAP application is designed for new Lenders and Servicers to enroll in the Federal Family Education Loans (FFEL) program. Prospective FFEL Lenders and Servicers access LAP to verify and update their demographic information in order to populate the Lender Reporting System (LARS). The representative uses the "enroll now" option to select the type of agency he is representing (i.e., Lender, Servicer, Lender/Trustee). Once the agency type has been selected, the representative is required to complete the LAP. Upon submission and approval confirmation e-mail is sent to the institution confirming their enrollment. Once the data is in LARS, representatives use the LARS profile functionality to make any future changes.

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 legal authority that allows FSA to collect privacy protected information in the IPM system is found in the Higher Education Act of 1965, Title IV, as amended, (20 U.S.C. 1088, 1094, 1099c) and the Debt Collection Improvement Act of 1996 (31 U.S.C. 7701).

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 IPM System contains information for individuals regarding the eligibility, administrative capability, and financial responsibility of postsecondary schools, lenders, guaranty agencies, or third-party servicers that participate in title IV, HEA student financial aid programs; such information includes, but is not limited to, the names, taxpayer identification numbers, bank account numbers, SSNs, personal identification numbers, personal addresses, personal phone numbers, and personal email addresses of the individuals with substantial ownership interests in, or control over, those entities. The IPM System also contains information about individuals affiliated with authorized entities (schools, lenders, guaranty agencies, and third-party servicers) that request electronic access to title IV, HEA Federal Student Aid systems. Such information includes, but is not limited to, the individual's name, SSN, date of birth, address, phone number, and authentication information (user ID, password, and security challenge questions and answers).

The sources of information are: Partner Demographics, Partner Official, Owners and FSA Internal Users. All information is collected using a secure website developed for IPM. Currently IPM houses all of its data in a single database and there is no linking or cross-referencing required.

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 will enable FSA to effectively administer Title IV partner eligibility, certification, and regulatory compliance. Additionally, this information will enable IPM to manage the partner enrollment, participation, and oversight processes. All the data collected by IPM is secured within the boundary of VDC, additionally, data is transmitted using Hypertext Transfer Protocol Secure (https); whether the data is collected using a browser or published or consumed via Windows Communication Foundation (WCF) web service.

To further mitigate privacy risks, External Users who are provisioned in IPM are vetted through SAM.gov debarment service to ensure the users are not debarred or suspended from conducting business with the Federal Government. Internal Users are allowed into IPM after they obtain clearance and approval from the ISSO during the provisioning process.

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 Social Security Numbers (SSN) are collected and used by IPM to perform the debarment process by checking user data against the debarment. SSNs are also used internally with FSA's Access and Identity Management system to ensure user uniqueness across FSA's enterprise systems. This is a business requirement and there are no other alternatives available to perform a debarment check without an SSN or Name.

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 contained in IPM is used for the purposes of determining initial and continuing eligibility, administrative capability and financial responsibility of postsecondary schools, lenders and guaranty agencies that participate in Title IV, HEA student assistance programs, and third-party servicers contracted by these entities; tracking changes to those entities; maintaining history of this information regarding entities that have ever applied to participate or participated in these programs; documenting any protective or corrective action against an entity or an individual associated with the entity; and establish the identity of individuals who request access to Title IV Student Aid Systems. The external sources of publicly available data for IPM are obtained from the following sites:

Source	Description
nces.ed.gov	a link is provided from IPM to nces.ed.gov for users to search and enter CIP codes for school programs
SAM.gov	IPM invokes a web service to ensure that each provisioned user is not debarred from conducting business with the Federal Government and/or any Federal Government Agency
Congressional Districts	To associate Partner Addresses with

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?

IPM will share Privacy data internally with FSA Access and Identity Management System (AIMS). AIMS is the enterprise security system for FSA and enforces security controls for IPM. User provisioning data provided by IPM will ensure each Partner user is mapped to a single unique identity across Federal Student Aid systems.
Privacy information will be shared and transmitted securely within the FSA Virtual Data Center (VDC) secured network and is only accessible by authorized administrators that have passed Department of ED security clearances. The specific information that will be shared with AIMS is listed below:

- First Name
- Last Name
- Social Security Number (SSN)
- Date of Birth
- Pseudo SSN (for foreign nationals)
- Email Address
- Phone Number

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?

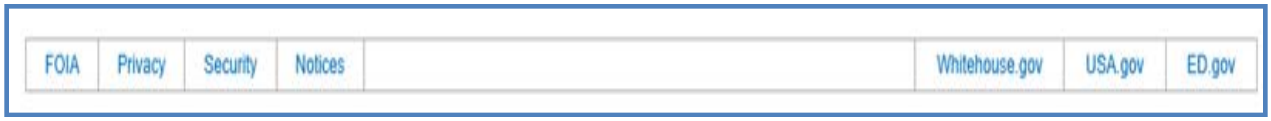
No, IPM system will not share Privacy data with external entities. IPM calls sam.gov web service and passes the user's First name, Last name and SSN to validate whether the user is debarred from doing business with any Federal Government Agency. This information is

transmitted using a secure web service and sam.gov only validates whether the user exist in the debarment database. Sam.gov does not store any information transmitted via the web service.

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 Policy and Statement is to be displayed on the IPM Portal informing users of the types of personal information that is to be collected by IPM, the authority under which that information is collected, that personal information provided to IPM is to be provided on a voluntary basis, and that information will only be shared with other organizations for purposes consistent with Section (b)(1) through (12) of the Privacy Act, as described under Question 4 above.

The policy highlights the voluntary nature of information collected, and describes the purposes for which the information is collected. The Privacy Policy and Statement informs users that providing the information constitutes consent to all of its uses and that they are given no option to affirmatively consent to specific uses. In addition, the policy notifies customers about the automatic recording and potential uses of any non-personal information about a visit (i.e., site management data). A link to the Privacy Act Statement is provided on each page of the IPM web portal on which the SSN is collected or displayed (see figure below). Users are specifically notified that providing the SSN is voluntary, but enrollment in IPM cannot be established without providing the SSN for this purpose.



Registering as a user with IPM is strictly voluntary. However, it is necessary for any institution wishing to participate in Title IV, student assistance programs to have a designated DPA enrolled as a DPA user with IPM. Such a designated DPA cannot be enrolled with IPM as a DPA user without providing the requested personal information. Likewise, IPM users are required to provide certain personal information on a voluntary basis. However, users will not be provided access to IPM if they choose not to provide the personal information requested.

The Privacy link on the IPM portal points to: http://www2.ed.gov/notices/privacy/index.html; which was provided by FSA.

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

http://www2.ed.gov/notices/privacy/index.html

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 Security Authorization been completed? Is the system compliant with any federal security requirements?

Note: IPM is still in the development phase. The IPM system has not completed the Security Authorization process. IPM Security Authorization will be completed before system goes into production.

Information contained within IPM is protected from unauthorized access by numerous security controls implemented within IPM as part of IPM development and deployment process. IPM security controls are fully described in the IPM System Security Plan, and are compliant with all Federal and Department of Education requirements for security in Federally-owned information systems and the data stored within those systems.

The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987." The IPM System's security plan demonstrates the IPM System's compliance with the IT security requirements mandated by Federal law and policy. The security plan contains details regarding the Risk Assessment conducted for the system, as well as the security controls (hardware/software/facilities/personnel) in place to mitigate any identified risks to the information collected by the IPM System. Management, operational, and technical security controls are in place for IPM, encompassing personnel, physical environment access, contingency plans, disaster recovery, and identification and authentication procedures.

The information collected and maintained by IPM, on behalf of the U.S. Department of Education, Office of Federal Student Aid, is secured using the requirements established by the Federal Information Security Management Act of 2002 (FISMA) and in accordance with NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, Revision 4, and NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.

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?

Yes. IPM is to be a System of Records as defined in Section (a)(5) of the Privacy Act. A System of Records Notice (SORN) is also being developed and will be submitted prior to system going live in September 1, 2017.

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:

Yes, the IPM system will record documents according to NARA Disposition Authority #: N1-441-09-15 / ED Schedule 074, which provides a common disposition for Federal Student Aid records related to oversight, compliance and improvement services; review report analysis; eligibility; recovery coordination; or monitoring the performance of schools that participate in the Title IV programs. This Disposition Authority is located at:
http://www2.ed.gov/about/offices/list/om/docs/rm-fsa-guaranty.pdf

The following is taken from the **IPM System and Supplemental Detailed Requirements Document (DRD)** version 1.4 dated 3/14/14

Table 1: Security & Privacy*: Security Policies High-Level Statements*

#	Requirement Definition	Source
SP-001	The IPM System shall adhere to FSA, NIST SP 800-37 C&A, and FIPS 200 requirements.	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-028)
SP-002	The IPM System shall implement NIST SP 800-53 Rev. 4 (Recommended Security Controls for Federal Information Systems and Organizations) controls according to its FIPS 199 classification.	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-028)
SP-003	The IPM System shall comply with the Computer Fraud and Abuse Act of 1987. http://cio.doe.gov/Documents/CFA.HTM	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-002)
SP-004	The IPM System shall comply with the Computer Security Act of 1987. http://www.epic.org/crypto/csa/csa.html	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-003)
SP-005	The IPM System shall comply with the Federal Information Security Management Act (FISMA) of 2002 (Title III of E-Gov). http://csrc.ncsl.nist.gov/policies/	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-005)
SP-006	The IPM System shall comply with the Privacy Act of 1974. http://www.ed.gov/policy/gen/leg/privacyact.html and Section 208 eGovernment Act of 2002	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-013)
SP-007	The IPM System shall comply with Executive Order 13231 - "Critical Infrastructure Protection in the Information Age". http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-015)
SP-008	The IPM System shall comply with Executive Order 13228 –"Establishing the Office of Homeland Security and the Homeland Security Council". http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-016)
SP-009	The IPM System shall comply with OMB Circular A -130 – "Management of Federal Information Resources", Appendix III – "Security of Federal Information Resources". http://www.whitehouse.gov/omb/circulars/a130/a130.html	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-020)
SP-010	The IPM System shall comply with U.S. Department of Education "Information Technology Security Manual".	SOO Tech Appendix (Section 5.1.8 Standards and Regulations) (SR-027)

#	Requirement Definition	Source
SP-011	The IPM System data shall be protected as defined by the guidelines set forth in FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems".	(TF-015)

Table 2: Security & Privacy*: Authorization Requirements*

#	Requirement Definition	Source
SP-014	The IPM system shall have the ability to exchange certifications with external systems.	Updated per meeting held 2/6/14 SOO Technical Appendix Addendum – Section 2.3 (High-Level Functional Requirements); 02/23/2011 DRD Review Meetings (Security&Privacy) (ORMS-16)
SP-015	The IPM System shall support the enforcement of fine grain access rights/privileges for IPM system users (as defined in the User Roles Matrix and DUC 2.1).	REQ-1.3; 02/23/2011 DRD Review Meetings (Security&Privacy)
SP-016	The IPM system shall enforce the principle of separation of duties when assigning user authorization (as defined in the User Roles Matrix, DUC 2.1 and DUC C06.3).	REQ – 7.; 02/23/2011 DRD Review Meetings (Security&Privacy) (AC5-1)
SP-017	The IPM system shall enforce access to information maintained in the IPM system through assigned authorization (as defined in the User Roles Matrix and DUC 2.1).	REQ – 6; 02/23/2011 DRD Review Meetings (Security&Privacy); REQ-13; 02/22/2011 DRD Review Meetings (AIM/IPM User Management) (AC4-1) (AC13-1)

Table 3: Security & Privacy: Miscellaneous Requirements

#	Requirement Definition	Source
SP-018	The IPM system shall have the capability to encrypt all PII data in transit and data at rest in accordance with the attached System Level PII data elements and DOE Encryption Safeguard Privacy doc.	Updated per meeting held 2/6/2014 02/23/2011 DRD Review Meetings (Security&Privacy)
SP-019	The IPM system shall support or contain automated mechanisms to prevent information, including encrypted representations of information,	REQ – 60.2

#	Requirement Definition	Source
	produced by the activity of a previous user or application process from being available to a successor user or application process that obtains access to a shared system resource. Shared system resources include main memory, secondary storage, registers and session credentials.	