Privacy Impact Assessment (PIA) for the
Financial Management System (FMS)

Nov 29, 2018

This PIA was originally approved on Jan 6, 2011 and reviewed on Dec 13, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Alonzo D. Posey, Information System Security Officer (ISSO)
Contact Email: fsacofmsgsecurityteam@ed.gov

System Owner

Name/Title: Milton L. Thomas Jr., Director, Financial Management Systems Group
Program Office: Federal Student Aid (FSA)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.
Please complete this Privacy Impact Assessment (PIA) on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. If a question does not apply to your system, please answer with N/A.

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

The Financial Management System (FMS) is a fully integrated financial management system, utilizing Oracle Federal Financials, which incorporates full financial business functionality, including general ledger (GL), accounts payable (AP), and accounts receivable (AR) across multiple FSA program areas. FMS supports FSA service areas, enterprise areas and partners, and provides timely and consistent financial data for strategic decision making. FMS provides FSA with a fully auditable accounting system incorporating appropriate security controls, and audit trails.

FMS only collects data directly from users to create a user ID to uniquely identify each customer who has been granted access to FMS. FMS does store PII data as it is received from other FSA, contractor-managed systems and trading partner systems, as well as organizations that support Title IV programs to perform essential business and customer functions, such as processing loans and grants and disbursements/collections.

1.2 Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained or shared.

The purpose for which the personally identifiable information (PII) is collected and used by FMS is to create a user ID to uniquely identify each customer who has been granted access to FMS. FMS also maintains and shares PII received from other FSA systems to perform essential business and customer functions, such as processing loans and grants, disbursements/collections, and to uniquely identify each customer.

1 The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
1.3 Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

Updated PIA  
Original Publication Date: 02/03/2017

1.5 Is the system operated by the agency or by a contractor?

Agency

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1 What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

FMS is considered a system of records under Privacy Act records and maintains records, and may disclose records to both the US. Department of the Treasury and to loan holders, under the following authority:


B. ECASLA of 2008 (Public Law 110-227) and 31 U.S.C. 7701 and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

SORN

2.2 Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer YES or NO.

Yes
2.2.1 □ N/A If the above answer is YES this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).² Please provide the SORN name and number, or indicate that a SORN is in progress.


Records Management

*If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov.*

2.3 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

The FMS is covered by the following NARA records schedule:
ED 069 Financial Management System, Item a, which is pending approval from NARA.
The retention is: Cut off annually when entity ceases participation in Title IV programs. Destroy/delete 15 years after cut off.

The FMS also utilizes NARA schedule:
ED 086 Information Systems Supporting Materials, Items a, b, and d; which follows General Records Schedule (GRS) 20 items 2, 10, and 11.

---

² A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED: [https://connected.ed.gov/om/Documents/SORN-Process.pdf](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer YES or NO.

Yes

3. Characterization and Use of Information

Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

FMS collects full name, job title, work location, email address, work phone number, supervisor's full name, job title, telephone number, email and signature, and status of user's Federal Student Aid Personnel Security Clearance (Clearance level and clearance type) as part of a request by a person to gain access to FMS. This information is used to generate a User ID to grant a requestor access to the system.

Only the name and email address is stored within the FMS System. FMS does store PII data it receives from other FSA, contractor-managed systems and trading partner systems, as well as organizations that support Title IV programs. See question 3.3 for a list of specific systems.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer YES or NO.

Yes

3.3 What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

FMS does not collect any data directly from users, but stores PII data as it is received from other FSA, contractor-managed systems and trading partner systems, as well as organizations that support Title IV programs. The list below provides a collection of systems with which FMS exchanges data:

A. Common Origination and Disbursement (COD) System,
B. Debt Management and Collection System (DMCS),
C. eCampus Based System (eCBS),
D. Department's Education Central Automated Processing System (EDCAPS), which includes the G5 and Financial Management System Software (FMSS),
E. Enterprise Data Warehouse and Analytics (EDWA),
F. National Student Loan Data System (NSLDS),
G. Postsecondary Education Participants System (PEPS),
H. Student Aid Internet Gateway (SAIG) mailboxes,
I. Title IV Additional Servicers (TIVAS), and
J. Loan-servicing companies, financial agencies, Federal, State, and local government agencies, and institutions of higher education.
3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

FMS does not collect any data directly from users (other than information need to grant a user access to FMS), but stores PII data as it is received from other FSA, contractor-managed systems and trading partner systems, as well as organizations that support Title IV programs. Records in this system are retrievable by name of borrower and address. Full FMS application functionality is available for FMS users through ED’s internal network or a virtual private network. Limited FMS application functionality is available to authorized trading partners via an external facing web server, but each can view or submit only their own data. FSA Title IV Additional Servicers (TIVAS) are allowed to view reports containing PII data for general ledger work-in-progress (WIP) and account Transfers In and Out transactions between servicers, but only for transactions they initiate or for which they are directly assigned.

3.5 How is this information validated or confirmed?

FMS depends on the input validation mechanisms provided by the systems that feed data into FMS.

---

3 Examples include form filling, account verification, etc.
Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The information contained in this system is maintained for the following purposes relating to students and borrowers: (1) to determine student/borrower eligibility for refunds of loan overpayments or loan discharges received by the Department's Office of FSA from individual borrowers participating in the Title IV, Health Education Act (HEA) programs; (2) to report information for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and discharges of Title IV, HEA, FSA; (3) to receive loan refund information and to send refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Department of the Treasury to the borrower; and (4) to receive financial records from Title IV servicers and Ensuring Continued Access to Student Loans Act (ECASLA) custodians that contain SSNs of the borrowers used specifically for the accounting of loans.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

Yes

3.7.1 N/A If the above answer is YES, what controls are in place to minimize the risk and protect the data?

1) Restricted access to the data, 2) Data is sanitized, 3)SFTP is used for file transfers. See response to question 7.3.
3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

Yes

3.8.1 □ N/A If the above answer is YES, please explain.

As part of the FMS release cycle, due to requirements with our partner systems, "live" PII is used in test data (i.e. DUNS/SSN info, Payee Name/Address/TIN/Bank Info) sent through secure file transfers between FMS and its partner systems to test and validate functionality. At the completion of each FMS release cycle, the development and testing environments are destroyed and rebuilt for the next quarterly release cycle.

Social Security Numbers

*It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

3.9 Does the system collect Social Security Numbers? Please answer YES or NO.

No

3.9.1 □ N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

FMS does not collect any SSNs directly from users, but stores PII data as it is received from other FSA, contractor managed systems and trading partner systems, as well as organizations that support Title IV programs. This PII data from other systems may include SSNs.
4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

There is a Privacy Act statement on the FMS User Access Request Package that all requesters must read and sign to acknowledge.

The systems that store PII on FMS provide notice to the public at point of collection. See the PIAs for those systems listed in 3.3 for additional information.
4.2 N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

The notice can be found on the FMA User Access request Package found at https://fp.ed.gov/fms.html

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The information collected directly by individuals is strictly voluntary giving individuals the option to decline or opt out.

For the information maintained in FMS but collected by other systems, please refer to the corresponding PIAs and SORNs for each respective system.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
5.2 N/A  What information will be shared and with whom?

Information in FMS is used for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and loan discharges of Title IV federal student aid. FMS receives loan refund information and sends refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Dept. of the Treasury to the borrower.

5.3 N/A  What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Information in FMS is used for the purpose of processing refunds to borrowers or loan holders (lenders and guaranty agencies) for overpayments and loan discharges of Title IV federal student aid. FMS receives loan refund information and sends refund transaction data files (the borrower's name and other identifiers) to the Department of Education's Central Automated Processing System (EDCAPS) for validation and subsequent payment by the Dept. of the Treasury to the borrower. The purpose aligns with the stated purpose in question 1.2 above.

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer YES or NO. If the answer is NO, please skip to Question 5.8.

Yes
What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

FMS exchanges data with the following external organizations (note: the list below is not all inclusive):
A. Title IV loan servicers
B. Loan-servicing companies,
C. Financial agencies,
D. Federal, state, and local government agencies,
E. Institutions of higher education, and
F. The U.S. Department of Treasury

FMS receives this information to conform to the standard Department of Treasury check/EFT layout (SF 1166 format) requirements for refund payment processing. The Department of Treasury may use the refund information in pursuing offsets against obligations owed to the Federal Government.

What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

FMS receives this information to conform to the standard Department of Treasury check/EFT layout (SF 1166 format) requirements for refund payment processing. The Department of Treasury may use the refund information in pursuing offsets against obligations owed to the Federal Government. The purpose aligns with the stated purpose in question 1.2 above.
5.7 N/A How is the information shared and used by the external entity?

External FMS users access the system utilizing Oracle Access Manager (OAM) to provide user authentication adding the ability for a two-factor authentication service using the user’s FMS password and registered token. Refer to question 1.2 for data use.

5.8 N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

No

5.9 N/A Does the project place limitation on re-disclosure? Please answer YES or NO.

Yes

6. Redress

6.1 What are the procedures that allow individuals to access their own information?

Procedures for allowing individuals to access their own information are explained in the System of Records notice listed in question 2.2. The SORN is located at: 73 Federal Register 177 - 179, (January 2, 2008) or at https://www.federalregister.gov/documents/2008/01/02/E7-25520/privacy-act-of-1974-system-of-records-financial-management-system-fms

4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.
6.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Procedures for allowing individuals to correct inaccurate or erroneous information are explained in the System of Records notice listed in question 2.2.

6.3 How does the project notify individuals about the procedures for correcting their information?

The System of Records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1 Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer YES or NO.

Yes
7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

Access to FSA information is governed by the concepts of least privilege and separation of duties. All system access is granted by predefined roles and privileges, and all FSA system users must undergo a Federal background security clearance process.

7.3 What administrative, technical, and physical safeguards are in place to protect the information?

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the Federal Information Security Modernization Act of 2014, 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. FMS received its ATO on 05/09/2018. 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, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

7.4 Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

See 7.3 above.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

The system owner participates in major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA’s Lifecycle Management Methodology, which addresses security and privacy risks throughout the system’s lifecycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of records notices, Trading Partner Agreements, etc.
Privacy risks of unauthorized disclosure of PU are mitigated by limiting access to FMS and, when appropriate, sanitizing the information once the transaction validation is completed. FMS has identified specific fields in each table that contain PII data and in the process of implementing Label Security & Data Masking in near future. All users of this system of records are given unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy (this policy requires a complex password that must be changed every 90 days). Annually, all users of FMS must acknowledge the completion of FMS-specific security awareness training before they can obtain or renew their access to the system. An automated audit trail documents user activity of each person and device having access to FMS. FMS has completed a formal security assessment and is now enrolled in Federal Student Aid's Ongoing Security Authorization (OSA) program. Under the OSA program, the FMS NIST 800-53 controls are continually assessed on a quarterly basis per an OSA security control test schedule. The results of the OSA security control tests are documented by Federal Student Aid (FSA)'s security control assessment team.