Privacy Impact Assessment (PIA)

for the

Financial Management System (FMS)

May 17, 2021

For PIA Certification Updates Only: This PIA was reviewed on **May 17, 2021** by **Alonzo D. Posey** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Clinton Swart/Information System Security Officer (ISSO)
Contact Email: fsacfofmsgsecurityteam@ed.gov

System Owner

Name/Title: Milton L. Thomas, Jr./Director, Financial Management Systems Group
Principal Office: Office of Finance and Operations (OFO)

Please submit completed Privacy Impact Assessments to the Privacy Office 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.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Financial Management System (FMS) is a fully integrated financial management system that uses Oracle Federal Financials to incorporate full financial business functionality, including general ledger (GL), accounts payable (AP), and accounts receivable (AR) across multiple Federal Student Aid (FSA) program areas. FMS is the single point of financial information by lender, servicer, and school institution, integrating transactions both from the FSA feeder systems as well as from the Grants Administration and Payment System (G5). Accordingly, FMS provides consolidated data to support key management analysis and is the only source within the U.S. Department of Education (Department) to obtain a comprehensive financial picture of an institution across all FSA programs.

FMS consolidates and manages all FSA program transactions from FSA's feeder systems (e.g., Federal Family Education Loan (FFEL), Direct Loan, Pell, and Campus-based transactions) and FSA's partner systems managed by the Title IV Additional Servicers (TIVAS) and Not For Profit (NFP) Servicers. These systems transfer functional transactions to FMS where they are translated to the appropriate accounting documents. FMS also tracks and manages the payment processing for direct loan originations and consolidations by G5 and processes refunds to borrowers for overpaid loans. In addition, FMS supports FFEL loans through customized extensions, integrated with the Oracle sub-ledgers, processing large volumes of payments to the lender and guarantee agency communities. It receives electronic invoices and advice of fees payable to the Department, performs complex custom validations and reasonability checks to minimize erroneous payments and processes the transactions through Oracle sub-ledgers to generate U.S. Treasury payment files and accounting transactions. Accounting transactions posted in FMS are, in turn, summarized and sent to the Financial Management Support System (FMSS), the core financial management system for external financial reporting.

FMS serves mission-critical functions as a FFEL program front-end payment system, to provide reconciliation to the FSA feeder systems, for the generation of detailed internal program management reporting, and to provide additional levels of system controls. However, FMS does not fulfill the central functions of a Federal Financial Management Improvement Act (FFMIA) core financial management systems. FMSS, not FMS, produces all external financial reports, such as the financial statements. In addition,

FMSS serves as the source for all budget funding transactions (appropriation, apportionment, and allotment data).

For a list of trading partner systems, see question 3.1.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained, or shared.

FMS collects and uses PII 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.

FSA Servicers send FMS the following PII borrower data to support payment files to the U.S. Treasury to refund overpayments from borrowers:

- borrower name
- address
- Social Security number (SSN)
- optional banking information (routing ID and bank account number)

FSA Servicers send FMS the following borrower data to reconcile loan disbursements between servicers and Common Origination and Disbursement (COD) and loan transfers between servicers:

- loan ID number
- SSN

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?

Updated PIA

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

[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. OMB Circular A-130, page 33

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☑ N/A

Click here to select.

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? Please include name and citation of the authority.

FMS maintains records and discloses records to both the U.S. Department of the Treasury and to loan holders, under the following authorities:

A. 20 U.S.C. 1070 et seq. Title IV of the Higher Education Opportunity Act (HEOA) (Public Law 110-315) enacted on August 14, 2008, which reauthorizes the Higher Education Act of 1965, as amended (HEA).

B. Ensuring Continued Access to Student Loans Act (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?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

[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

Financial Management System (FMS) (18-11-17), as published in the Federal Register on January 2, 2008 at 73 FR 177.

An updated FMS SORN is in progress.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

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. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

FMS is covered by the following NARA records schedules:
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.

ED 086 Information Systems Supporting Materials, Items a, b, and d; which follows General Records Schedule (GRS) 20 items 2, 10, and 11.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

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

A. FMS collects contact information from users (Federal employees and contractors) to create access credentials. The complete list of data elements FMS collects is as follows in order to provide access to the system: full name, job title, work location, email address, work phone number, supervisor's full name, job title, telephone number, email address, signature, and status of user's FSA Personnel Security Clearance (clearance level and clearance type). This information is used to generate a user ID to grant a requestor access to the system. Only the name and email address are stored within the FMS system.

B. FMS collects from FSA servicers the following borrower data to support payments to the U.S. Department of the Treasury. The purpose is to refund overpayments from borrowers:
   a. borrower name
   b. address
   c. SSN
   d. optional banking information (routing ID and bank account numbers)

C. FMS collects from FSA servicers the following borrower data elements in order to reconcile loan disbursements between servicers and COD and loan transfers between servicers
   a. loan ID
   b. SSN

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes – Data collection practices are listed below:

- User Provisioning – Data elements collected are required to complete user provisioning in a High-Value-Asset (HVA) system and comply to best practices in determining clearance and level of access.
- Borrower Refund payment-Data collected to support borrower refund payments is required by the U.S. Treasury Bureau of Fiscal Service and the Internal Revenue Service.
- Loan Booking reconciliations- Data collected are the minimum data point to reconcile individual loan booking between servicers and COD permitting control within this financial activity.

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

FMS collects data directly from FMS users for account creation. However, FMS also stores PII it receives from other FSA contractor-managed systems and trading partner systems. The list below provides a collection of systems with which FMS exchanges PII data:
A. Common Origination and Disbursement (COD) System,
B. Debt Management and Collection System (DMCS),
C. Department's Education Central Automated Processing System (OCIO-EDCAPS), which includes the Grants Management System (G5) and Financial Management support System (FMSS),
F. Student Aid Internet Gateway (SAIG) mailboxes,
G. Title IV Additional Servicers (TIVAS), and Not for Profits

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

FMS User Provisioning – Users submit User Request Access forms by email to the FMS Helpdesk. The forms are scanned for review and processing.

The list below provides description on how FMS exchanges PII data between system:
A. Common Origination and Disbursement (COD) System –
    a. RECON PROCESS- Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).
B. Debt Management and Collection System (DMCS)-
    a. RECON PROCESS Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).

b. BORROWER REFUND- Sent by interface file (FMS REFUND) via SAIG

C. Title IV Additional Servicers (TIVAS), and Not for Profits –
   a. RECON PROCESS Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).
   b. BORROWER REFUND- Sent by interface file (FMS REFUND) via SAIG

D. Department's Education Central Automated Processing System (OCIO-EDCAPS), which includes the Grants Management System (G5) and Financial Management support System (FMSS), - Collected Refund payment files through Secure File Transfer protocol (SFTP) to move to U.S. Treasury (OFO holds Treasury Warrant).

E. Student Aid Internet Gateway (SAIG) mailboxes,- Is an encrypted transfer medium.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Information collected from individuals to gain access to the FMS system is validated and confirmed to ensure its integrity by the Information Systems Security Officer (ISSO) and reviewed by the FMS Helpdesk Operations staff as part of the Quality Analysis (QA) process. This validation includes a review of all data elements, accurate acknowledgement of Security Awareness training, acknowledgement of internal and external rules of behavior and a validated proper signature of the individual and their supervisors. This process is performed daily for each FMS User Access Form submitted.

Input validation is performed by each system that feeds data into FMS to validate/confirm the integrity of their PII. In addition, FMS validates fields for proper data field type, nomenclatures and size. Please refer to the PIAs for the other Department systems listed in question 3.3 for information about how data is validated in FSA partner systems.

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The information contained in this system is maintained (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's EDCAPS system for validation and subsequent payment by the U.S. 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 system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

Yes

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

☐ N/A

1) Restricted access to the data, 2) Data stored on memory devices are sanitized, 3) Secure File Transfer Protocol (SFTP) is used for file transfers. Data are encrypted both at rest and in transit.

See the response to question 7.4 for an additional description of security and privacy controls that apply to the data in the system.

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.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

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

FSA Servicers send FMS the following PII borrower data to support payment files to U.S. Treasury to refund overpayments from borrowers:

- borrower name
- address
- SSN
- optional banking information (routing ID and bank account number)

FSA Servicers send FMS the following borrower data reconcile loan disbursements between servicers and COD and loan transfers between servicers:

- loan ID and SSN

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

SSN is required by the U.S. Department of the Treasury for issuing borrower payments. No alternatives exist.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? 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. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

The notice can be found on FSA/FMS Security Forms at https://fsapartners.ed.gov/knowledge-center/topics/financial-partners

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, 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.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

F. Common Origination and Disbursement (COD) System – **SSN, Loan ID**
   a. RECON PROCESS- Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).

G. Debt Management and Collection System (DMCS)- **SSN, Loan ID, Borrower Name, Borrower Address, Banking Info (optional)**

a. RECON PROCESS Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).
b. BORROWER REFUND- Sent by interface file (FMS REFUND) via SAIG

H. Title IV Additional Servicers (TIVAS), and Not for Profits – **SSN, Loan ID, Borrower Name, Borrower Address, Banking Info (optional)**
   a. RECON PROCESS Reported through the Work-In-Process, Transfer-in, Transfer-out reporting by database flat-file exchange (VIA SAIG).
   b. BORROWER REFUND- Sent by interface file (FMS REFUND) via SAIG

I. Department's Education Central Automated Processing System (OCIO-EDCAPS), which includes the Grants Management System (G5) and Financial Management support System (FMSS) - **SSN, Borrower Name, Borrower Address, Banking Info (optional)**
   a. Collected Refund payment files through Secure File Transfer protocol (SFTP) to move to U.S. Treasury (OFO holds Treasury Warrant).

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

FMS is sharing the specified PII with DMCS, TIVOS, and NFPs to facilitate refunds on borrower overpayments.

FMS is sharing PII with COD and Servicers/DMCS to perform financial reconciliations as a control on loan disbursement and bookings.

In addition, shares PII data with FMSS for validation and subsequent payment transmittal to the U.S. Department of the Treasury.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

FMS exchanges PII between Title IV loan servicers, NFPs, DMCS and COD to reconcile loan balances (internal) with the U.S. Department of the Treasury via EDCAPS to process borrower refunds (external).

FMS exchanges PII between Title IV loan servicers, NFPs, DMCS and FMSS To issue refund loan overpayments back to the borrower or loan holder and to answer questions that may arise about the refund payments, the FSA disclose information from this system to the Department of the Treasury via Treasury's Electronic Certification System (eCS).

The only external party FMS exchanges is the U.S. Treasury Bureau of Fiscal Service via an SFTP transfer to FMSS. Note: Treasury Warrant for payments are not held by FSA

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

FMS shares this information to conform to the standard U.S. Department of the Treasury check/Electronic Fund Transfer (EFT) layout (Standard Form 1166 format) requirements for refund payment processing. The U.S. Department of the Treasury may use the refund information in pursuing offsets against obligations owed to the Federal Government.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☐ N/A

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.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

No

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

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

Per the SORN listed in question 2.2.1, if someone wants access to a record in this system of records, they must provide the FMS system manager with their name, date of birth, and SSN. Requests for access to a record must meet the requirements of 34 CFR 5b.5, including proof of identity.

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.

Per the SORN listed in question 2.2.1, if someone wishes to contest the content of an FMS record, they must contact the system manager. Requests to correct or amend a record must meet the requirements of the regulations in 34 CFR 5b.7, including proof of identity, specification of the particular record that someone is seeking to have changed, and the written justification for making such a change.

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

The system of records notice listed in question 2.2.1 and this PIA 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?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. 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), as amended by the Federal Information Security Modernization Act of 2014, every FSA system must receive a signed authorization 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.

. FMS Uses the FMS Oracle EBS suite Oracle User Management, Its Core security includes Oracle's Function and Data Security models, as well as Role Based Access Control.

Function Security is the base layer of access control in Oracle E-Business Suite. It restricts user access to individual menus and menu options within the system, but does not restrict access to the data contained within those menus.

Data Security is the next layer of access control. Building on Function Security, Data Security provides access control within Oracle E-Business Suite on the data a user can access, and the actions a user can perform on that data. Oracle E-Business Suite restricts access to individual data that is displayed on the screen once the user has selected a menu or menu option.

Role based access control (RBAC) is the next layer and builds upon Data Security and Function Security. With RBAC, access control is defined through roles, and user access to Oracle E-Business Suite is determined by the roles granted to the user. Access control in Oracle E-Business Suite closely follows the RBAC ANSI standard (ANSI INCITS 359-2004) originally proposed by the US National Institute of Standards & Technology (NIST), which defines a role as "a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role."

Additional examples of specific controls include multifactor authentication, encryption of data at rest and in transit, firewalls, event monitoring systems, penetration testing, system audits, user recertification, and threat management. Finally, all privileged users are provided a copy of the Rules of Behavior and are required to complete the annual Cybersecurity and Privacy Awareness training.

Except for payee name only masked PII is used for testing when required. The frequency of such use is 1 out of 4 releases in a fiscal year. When PII is used for testing approval from the FMS ISSO is required.
The PII data is masked in all non-production environments so that it is protected from access by staff who do not have the appropriate access roles. This is done during the process of cloning the data set and the masking schema is verified during the 'functional validation'. Functional validation includes review of PII data tables and review of the

updated fields set during the clone to defaulted values. The environment is released for internal testing after 'functional validation'.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

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

FMS is enrolled in the FSA's Ongoing Security Authorization (OSA) program. Under the OSA program, the FMS security controls are continually assessed on a quarterly basis per the OSA security control test schedule. Some of the activities that are being conducted are scans to monitor, test, or evaluate central processing unit (CPU) patching, annual penetration testing, and pre- and post-maintenance release activities.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, the Privacy Act and the published SORN, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system.

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 and trading partner agreements.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks include unauthorized disclosure of PII, which could lead to identity theft and loan fraud. Additional risks include unauthorized modification of data, which could lead to erroneous loan servicing.

Privacy risks of unauthorized disclosure of PII 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.

All FMS users are given a unique user identification and must establish a password that adheres to the FSA 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 is enrolled in FSA's Ongoing Security Authorization (OSA) program. Under the OSA program, the FMS security 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 FSA's security control assessment team.