Privacy Impact Assessment (PIA)

for the

Federal Student Aid Loan Servicing

February 13, 2024

Point of Contact

Contact Person: Brunhilda Enwe Eya
Title: Information System Security Officer (ISSO)
Email: Brunhilda.Eya@ed.gov

System Owner

Name: Jeremy Dick
Title: Information System Owner (ISO)
Principal Office: Federal Student Aid

Submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

Federal Student Aid (FSA), as part of the student aid program authorized by Title IV of the Higher Education Act of 1965 (HEA), uses third-party servicers to support the management of the repayment and collection of loans and grant overpayments for aid provided to recipients.

The servicers support user account management to allow for aid recipients to view and make loan payments, view account status, calculate repayment schedules, and apply for deferment and forbearances.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

Loan transaction information is transmitted through pay.gov via secure file transfer protocol (FTP) to the U.S. Department of the Treasury which is reconciled (ongoing evaluation audit to ensure financial actions are done appropriately) via the Financial Management System (FMS). FMS contains summary accounting for loans and other loan-related transactions such as loan consolidation payment requests and refund payment requests as well as information on loans transferred from servicers.

Servicer communication with aid recipients may be performed through physical mail, email, web chats, phone calls, and via electronic signature processing for completion of appropriate forms. Servicing functions also include the posting of payments and reporting loan balances to FSA, along with assisting aid recipients regarding loan processing, deferments, and forbearance options.

The servicers exchange data with other FSA systems (see list below) on a weekly and/or monthly basis (as required based on financial reporting requirements) to ensure accurate reporting of loan balances and grant information or to transfer defaulted loans from FSA

to the servicer to support collection efforts. To ensure collection on loans, the servicer may perform validation checks on aid recipient contact information through skip tracing[1]entities along with reporting to credit bureaus. Additional reporting may occur to educational and lending institutions as well as other loan servicers to confirm loan balances and student enrollment status. Reporting may also occur to other government agencies such as State attorneys general, the Consumer Financial Protection Bureau, and the U.S. Department of Education's (Department's) Office of Inspector General, to support fraud investigations.

All servicer systems are hosted on their own domains, using a single sign-on via FSA ID for aid recipients and Personal Identity Verification (PIV) for servicers' contractors.

To service the loans on behalf of FSA, each servicer's system uses a customer-facing website and backend databases that are part of the system boundary. Each servicer's website allows aid recipients to access loan-level information and make updates to their accounts. The databases are used to store aid recipients' loan information. PII is shared with other FSA systems (listed below) via two methods, both facilitated by FSA's Student Aid Internet Gateway (SAIG): secure encrypted data transmission for external agency transfers and the SAIG mailbox system for FSA-managed systems.

Below is the list of servicers:

1. Maximus Education LLC/Aidvantage (ADVS)
2. Nelnet Diversified Solutions LLC (NLCS)
3. EDFinancial Services LLC (EDF)
4. Missouri Higher Education Loan Authority (MOHELA)
5. Central Research Inc. (CRI)
6. Perkins (Perkins)

Servicers transmit encrypted loan information with the following FSA systems:

- Common Origination and Disbursement (COD) – servicers use this system to obtain originating loan disbursement and cancellation details, as well as report transfer information for future loan assignments.
- Debt Management Collections System (DMCS) – servicers assign loans that have been delinquent for 360 days to this system, recall loans that were erroneously determined to be 360-days delinquent, and receive rehabilitated loans from DMCS.
- FMS – servicers report all financial transactions to FMS.
- National Student Loan Data System (NSLDS) – servicers use this system to obtain and report information for all stages of the loan cycle.
- FSA Partner Connect – servicers use this system to determine the current status of all schools participating in Title IV programs.

[1] Skip tracing is the process of tracking down aid recipients who are missing, unresponsive, or hard to find.

- Student Aid Internet Gateway (SAIG) – servicers use this system to receive and/or send data to multiple FSA systems.
- Other servicers - servicers transfer information pertaining to aid recipients' account history to other servicers if aid recipients' accounts are transferred to another servicer.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[2] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., parents, Federal employees, contractors), specify the purpose for each type of individual.

Information is collected to uniquely identify individuals to service their student loans. Servicers use this information to store, retrieve, and manage loan payments and balances. This information may be collected as part of the student loan application as well as the processing, collection, and disposition of aid recipients' accounts. This information is also used for individuals to electronically sign forms associated with management of their loan payments.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☐ N/A

[2] 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

Servicers are contractors that support the day-to-day operations of their respective systems, engage in loan servicing, and maintain all backend equipment utilized to support their systems.

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

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

Title IV of the Higher Education Act of 1965, as amended (HEA) (20 U.S.C. 1070 et seq.). The collection of SSNs of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled "Common Services for Borrowers," 18-11-16, 88 FR 48449, was last published in the Federal Register on July 27, 2023.

Aid recipient **Records Management**

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

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information. List the schedule(s):

Department Records Schedule No. 075 (N1-441-09-16), "FSA Loan Servicing, Consolidation, and Collections Records."

For servicers that are also servicing Health Education Assistance Loans (HEAL): DAA-0441-2017-0002, " FSA Health Education Assistance Loan (HEAL) Program Online Processing System (HOPS)."

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes
☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☒ Gender or Sex
☒ City, State, or County of Birth	☐ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☒ Personal Email Address
☒ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☒ Digital Signature ☒ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☒ Citizenship and/or Alien Registration Number (A-Number)	☒ Military Service	☒ Marital Status, Spouse, and/or Child Information (Specify below)
☒ Educational Background/Records	☐ Group/ Organization Membership	☒ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☒ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☒ Credit/Debit Card Number	☒ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☐ File/Case ID Number	☒ Federal Student Aid Number
☐ Student ID Number	☒ Student Loan Number	☒ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☒ Username/User ID	☒ Password	☒ IP Address

☐ MAC Address	☒ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☒ Location Data	☒ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☒ Other (Specify below)

If you have been directed to "specify below," describe the PII:

Information pertaining to complaints regarding services provided by customer service representatives (CSRs). This information includes the nature of the complaints, the CSR's name, and other pertinent details about the compliant.

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☐ Federal Employees

Specify types of information collected from Federal employees:

☐ Federal Contractors

Specify types of information collected from Federal contractors:

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, State, and local government employees), and the types of information collected from each:[3]

Aid Recipients:

[3] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.

The information collected includes city, state, educational status, family income, name, Federal student account number (FSA ID), date of birth (DOB), home address, permanent mailing address(es), email address(es), and telephone number(s) of the individuals obligated on the debt, bank account balance and asset information, recent tax documents (if applicable), employment status, employment verification, employer information, and income verification.

Valid identification (including birth certificate, court decree or court order supporting a name change, marriage certificate, U.S. Military discharge papers, credit score and history, military service information, area of study, marital status, number of dependent(s), educational background, race/ethnicity, student loan number, username/user ID, IP address, password, location data (for website metrics) and log data that can be traced to individual are also collected.

For aid recipients approved for automated payments, bank account number and debit card information will also be collected.

Co-aid recipients and cosigners:

The information collected includes name, DOB, household income, home address, permanent mailing address, email address, telephone number of the individuals obligated on the debt or whose income and expenses are included in a financial statement submitted by the aid recipients, work phone number, bank account balance and asset information, recent tax documents (if applicable), employment data, income verification, valid identification, credit score and history, military service information, marital status, dependent information, and race/ethnicity.

For co-aid recipients and cosigners assisting in payments, bank account number and debit card information will also be collected.

References:[4]
Name, relationship to aid recipient, address, phone number, email address.

Third-party preparers, endorsers:
Name, relationship to aid recipient, address, phone number, email address.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

Information is obtained from the aid recipients, co-aid recipients, cosigners, third-party preparers, endorsers, references provided by the aid recipients, commercial entities, other Federal agencies, and other FSA systems.

[4] References are able to verify information provided by aid recipients, co-aid recipients, and/or cosigners if need be.

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

The information is collected via the following channels:

- Phone calls, emails, and web chats with CSRs.
- Entries via interactive voice response (IVR) telephone services.
- Incoming paper correspondence (e.g., via physical mail).
- Aid recipients' use of servicers' websites.
- Secure data transmission within FSA systems (COD, DMCS, FMS, NSLDS, Partner Connect, SAIG, and other servicers).
- Secure data transmission with skip tracing vendors or person locator services to locate individuals. Once located, these entities will provide up-to-date information to the Department.
- Secure data transmission with the U.S. Postal Service (USPS) to obtain forwarding addresses.
- Secure data transmission from the Treasury for payment processing via Pay.gov, Intra-Governmental Payment and Collection (IPAC), collection of Internal Revenue Service (IRS) refunds, and revisions for aid recipient PII updates. IPAC is the mechanism used by the servicers to manage payments that are then sent to the IRS. If an aid recipient is defaulted on their student loans, payment can be taken from their IRS refunds.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

The information collected in 3.1 is the minimum necessary to enable effective loan processing and servicing activities. The information provided to the servicers allows for the effective management of the collection of loans, as well as grant overpayments, for aid provided to recipients.

Biographical and Contact Information:

- Aid recipients' name and DOB are needed to identify the aid recipient and to exchange data as necessary with other FSA systems and with external systems.
- Home address, phone number, and email address are used to contact the aid recipient if/when needed.
- Gender or sex, and country of birth (for verification of citizenship eligible non-citizen status) is are required to be included in the FAFSA by the FAFSA Simplification Act for individuals to be eligible for Federal student aid.
- Work address is collected from co-aid recipients and co-signers to confirm the income and expenses included in the financial statement submitted by the aid recipients.

Other Demographic Information:

- Citizenship and/or Alien Registration Number (A-Number) is required to identify the aid recipient for the purpose of approving the student loan.
- Military service information is required to identify any student loan benefits for members of the United States Armed Forces.
- Marital status, spouse, and/or child information is required to note dependency status and income level.
- Employment information is required to verify employment to assist in determining PSLF eligibility.
- Race/ethnicity is required to be included in the FAFSA by the FAFSA Simplification Act for individuals to be eligible for Federal student aid.
- Educational background/records is required to establish the aid recipient's eligibility based on their educational level.

Identification Numbers:

- Identification numbers such as the SSN, is required to accurately identify the aid recipients, co-aid recipients, and cosigners.
- For aid recipients approved for automated payments, bank account number and debit/credit card information are used to process payments.
- Student loan number and grant number are unique for each aid recipient and used to identify loan information.

Electronic and Miscellaneous Information:

- Usernames and passwords are stored within the system for access management and user authentication.
- Location data, IP address, and log data are collected for website metrics and to determine users are not accessing systems from unauthorized countries.

Complaint Information:

- Complaint information pertaining to complaints regarding services provided by CSRs, including the nature of the complaints, CSR names, and other pertinent details about the compliant are collected to investigate and adjudicate complaints. This information is needed to improve customer service.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☒ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches

previously collected information, account verification, periodically requesting system users verify their own information in the system)?

PII is directly received from aid recipients during the loan application process by other FSA systems, where system checks occur for data accuracy, prior to being sent to the servicers. PII is used to authenticate users during online account creation for access to servicer portals and telephone calls. If an aid recipient notes that the PII the servicer maintains about them is incorrect, records are updated within the respective system(s). Additionally, PII updates will occur because of information provided by other FSA systems, skip tracing, Directory Assistance and the National Change of Address Database (both maintained by the the U.S. Postal Service (USPS) to obtain forwarding addresses), and other third parties (e.g., educational institutions, financial institutions, loan servicers and consumer reporting agencies, and Federal agencies (e.g., Treasury)).

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.9 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☑ N/A

Click here to select.

3.8.2. If the above answer to question 3.9 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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 IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

The collection of SSNs of users of this system is authorized by 31 U.S.C. 7701 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

The SSN is the unique identifier for Title IV programs and its use is required by program participants and external partners to satisfy aid recipient eligibility, loan servicing, and loan status reporting requirements. The SSN is used for the following functions:

- To uniquely identify an individual within servicer systems.
- To uniquely identify an individual during the exchange of information between servicers and its external partners (e.g., Federal agencies, educational institutions, financial institutions, loan services, and consumer reporting agencies) that is performed in association with the servicing of the loans.
- To locate an individual for skip tracing purposes, report delinquencies to credit bureaus, and collect on the loans in case of delinquency or default.

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

SSNs are required for the purpose of validating a user's identity. SSNs are also used to match records as part of computer matching programs with other Federal agencies. Servicers also share SSNs as the unique identifier to help with skip-tracing tasks and to report to collection bureaus when delinquent. If individuals decline to provide their SSN, that will prevent the individuals' student aid application from being submitted or processed and affect the possibility of receiving student aid.

3.9.4. If the above answer to question 3.10 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

Alternatives to using SSNs have been considered but were determined not to be feasible due to the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA relies on SSNs to identify and track Federal student aid applications across systems internal and external to the Department.

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

A Privacy Act Statement is provided before the student or parent completes the Free Application for Federal Student Aid (FAFSA). This notice is provided both on the studentaid.gov website and the paper version of the FAFSA.

For servicers acting on the behalf of the Department, there are privacy policies located within each respective servicer's website. To establish an online account with specific servicers, the aid recipient must agree to the "Terms of Service," which incorporate the privacy policy by reference and link.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

☐ N/A

Yes

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☐ N/A

The FAFSA Privacy Act Statement can be found embedded in the Privacy Policy for StudentAid.gov.

Servicers: To view the privacy policies for each servicer, please refer to the websites provided on the list of servicers, found at: https://www2.ed.gov/notices/pia/tivas-nfp.docx.

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Aid recipients may decline to provide information; however, providing certain information is required to communicate with websites or customer service call centers and/or receive benefits on a loan such as deferment, forbearance, discharge, or forgiveness.

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

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

Yes

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☐ N/A

If information from a servicer is required in support of an investigation, resulting from information sent to the ODAS from the FAFSA Processing System (FPS), additional information from the servicers may be required. Information shared with the OIG may include any information associated with an aid recipient's loan. This information is used to support OIG field agents who are investigating aid recipients for potential fraud.

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☐ N/A

Records are shared with OIG to assist in investigating fraud. For more information on the uses of ODAS, please refer to the PIA for ODAS.

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

Servicers may share information with the following external entities:

- Skip tracing vendors or person locator services to locate individuals.
  - Name, DOB, address, city, State, personal phone number, work number, email address.
  - Example of a vendor that a servicer would use for skip tracing is Accurint/Lexis Nexis.
- Other third parties as authorized by consent of the aid recipient (e.g., employers, references).
  - Name, DOB, address, city, State, personal phone number, work number, email address.
- USPS for directory assistance and the National Change of Address Database to obtain forwarding addresses.
  - Name, address, city, State, phone number, email address.
- Institutions of higher education (IHEs) to coordinate the management of the loan with the institution's financial office.
  - Name, SSN, address, city, and State.
- Credit bureaus to update loan payment status.
  - Name, DOB, SSN, address, city, State, personal phone number, work number, email address.
- Treasury for payment processing via Pay.gov, IPAC, collection of IRS refunds, and revisions for aid recipient PII updates.
  - Name, SSN, address, city, State, personal phone number, email address.
- IRS for tax purposes and to process refunds.
  - Name, SSN.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

The information is shared for the following reasons:

- Skip tracing vendors or person locator services to locate individuals.
- Other third parties as authorized by consent of the aid recipient (e.g., employers, references).
- Digital signature vendors to assist in the signature process for official documents.
- USPS for directory assistance, and the national change of address database to obtain forwarding addresses.

- IHEs to coordinate the management of the loan with the institution's financial office.
- Credit bureaus to update loan payment status.
- Treasury for payment processing via Pay.gov, IPAC, collection of IRS refunds, and revisions for aid recipient PII updates.
- IRS for tax purposes and/or to process refunds.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

Title IV of the HEA, as amended (20 U.S.C. 1070 et seq.)

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

Yes

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

Yes

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

PII is shared externally via two methods, both facilitated by FSA's SAIG: secure encrypted data transmission for external transfers, and the SAIG mailbox system for FSA-managed systems.

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

☐ N/A

Yes

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

To gain access to a record in this system, requesters must provide the system manager with name, date of birth, and SSN. Requests by an individual for access to a record must meet the requirements of the regulations in 34 CFR 5b.5, including proof of identity.

In addition, aid recipients may access their own information via a website at the following locations:

- https://studentaid.gov/manage-loans/default
- https://myeddebt.ed.gov
- https://studentaid.gov/

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

If an individual wishes to contest the content of a record in this system of records, he or she should contact the system manager with name, date of birth, and SSN; identify the specific items to be changed; and provide a written justification for the change. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

In addition, aid recipients may access their own information to correct any inaccurate or erroneous information via the websites listed in question 6.1.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

This PIA, as well as the SORN listed in question 2.3, details the procedures for correcting customer information. FSA's website also provides access and correction 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 ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

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

Servicers' systems are located in one or more of their secure data center facilities. Access to servicers' systems is limited to servicers' employees, FSA employees, authorized IT professionals working on servicers' systems, and contractor program managers who have responsibilities for servicers' systems at hosting locations. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, servicers' systems must receive a signed ATO from a designated Department authorizing official. Security and privacy controls implemented for servicers' systems are comprised of a combination of administrative, physical, and technical controls.

Physical access to the servicers' sites, where their systems are maintained, is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge. Annual security and privacy training is required to ensure that individuals are appropriately trained in safeguarding these data. Servicers' systems offer a high degree of resistance to tampering and circumvention through the application of security controls. These controls limit data access to individuals on a "need-to-know" basis and control individual users' ability to access and alter records within the system.

All users accessing the system are given unique user identification. The servicers' systems require the enforcement of a complex password policy and two-factor authentication. In addition to the enforcement of the two-factor authentication and complex password policy, users are required to change their password at least every 90 days in accordance with the Department's IT standards. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

8. Auditing and Accountability

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

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, 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 all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology (LMM), 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 CMAs, memorandums of understanding (MOUs), and other information sharing agreements.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

The system owner in coordination with the Information System Security Officer (ISSO) and FSA Assessment Team ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system.

The servicers are enrolled in the FSA's Ongoing Security Authorization (OSA) program. Under the OSA program, the servicers' security and privacy 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.

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

Privacy risks associated with this system include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII and credentials are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, utilizing least privilege principles, masking SSNs, encrypting data in transmission, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by regularly updating security patches and device operating software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.