Privacy Impact Assessment (PIA)
for the

Title IV Additional Servicers and Not-for-Profit Servicers
June 22, 2022

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Greg Plenty, Supervisor, Technology Directorate
Contact Email: Gregory.Plenty@ed.gov

System Owner

Name/Title: Shital Shah/Information System Owner
Principal Office: Federal Student Aid (FSA)

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.

Federal Student Aid (FSA), as part of the Title IV student aid program authorized by the Higher Education Act of 1965 (HEA), as amended, uses servicers to support the management of the collection of loans, as well as grant overpayments, for aid provided to borrowers and grantees. Servicers are commonly referred to as Title IV additional servicers (TIVAS) and not-for-profit servicers (NFPs). The servicers support user account management for borrowers to view and make loan payments. Servicer communication with borrowers may be performed through U.S. 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 borrowers around 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 borrower contact information through collections and skip tracing 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 Department's Office of Inspector General, to support fraud investigations.

To service the loans on behalf of FSA, each servicer's system uses a customer-facing website and backend databases that are part of their system boundary. The website allows customers to access loan-level information and make updates to their accounts. The databases are used to store borrowers' loan information.
Below is the list of servicers and the names of the FSA systems to which the servicers transmit encrypted loan information:

1. Pennsylvania Higher Education Assistance Authority (PHEAA): Debt Management Collection System (DMCS), National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), Financial Management System (FMS), Missouri Higher Education Loan Assistance Authority (MOHELA), and Postsecondary Educational Participants System (PEPS).
2. Department of ED/Perkins (Perkins): DMCS, NSLDS, and FMS.
3. Aidvantage (ADVS): DMCS, NSLDS, COD, FMS, and PEPS.
4. Great Lakes Commercial System (GLCS): COD, DMCS, Digital Customer Care (DCC,) FMS, PEPS, and NSLDS.
5. Nelnet: COD, DMCS, DCC, FMS, PEPS, EdFinancial, Oklahoma Student Loan Authority (NFPOSLA), and NSLDS.
6. EdFinancial: DMCS, COD, FMS, Nelnet, PEPS, and NSLDS.
7. MOHELA: COD, FMS, PHEAA, PEPS, and NSLDS.
8. NFPOSLA: Nelnet.

For a complete list of the servicers please refer to the following link.

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

PII is collected and used in connection with loan processing and servicing activities: 1) to determine a student's eligibility for Title IV funds, 2) to account for Title IV funds, 3) to deliver Title IV funds to students, or 4) to perform any other aspect of the administration of the Title IV programs. Additionally, the PII is used for identification of loan and/or individuals between FSA and external systems as part of the data sharing process.

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?

[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

Updated PIA

The PIA is being updated as part of the required biennial review.

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

Contractor

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

☐ N/A

Yes

For further information related to contractor requirements, refer to the following link: http://www.ed.gov/fund/contract/about/bsp.html

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.

- The Higher Education Act of 1965 (HEA), as amended, Section 441 and 461 Title IV, Section 401.
- 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 (SSN) or other identification?

Yes

For management of collection of loans and grant overpayments for aid, information is retrieved by the SSN, date of birth, and name.

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

Servicers are covered under the "Common Services for Borrowers" System of Records Notice (SORN), which was published as number 18-11-16 in the Federal Register on September 2, 2016 (81 FR 60683).

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

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.

This system is under review for its revised record retention and subsequent NARA approval. Records will be safeguarded as permanent pending NARA approval.

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.

[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

Servicers collect and maintain the employment information (employer name, address, and employment status), educational status, family income, SSN, first and last names, Federal student account number, date of birth, permanent mailing address(es), email address(es), and telephone number(s) of the individuals obligated on the debt or whose income and expenses are included in a financial statement submitted by the borrowers. For borrowers approved for automated payments, bank debit card information will also be collected.

Records also include, but are not limited to: the application for, agreement to repay, and disbursements on the loan, and loan guaranty, if any; the repayment history, including deferments and forbearances; claims by lenders on the loan guaranty; and cancellation or discharges on grounds of qualifying service, bankruptcy discharge, disability (including medical records submitted to support application for discharge by reason of disability), death, or other statutory or regulatory grounds for relief.

Additionally, for Title IV HEA grant overpayments, the system contains records about the amount disbursed, the school that disbursed the grant, and the basis for overpayment. For all debts, the system contains demographic, employment, and other data on the individuals obligated on the debt or provided as references by the obligor, and the collection actions taken by any holder, including write-off amounts and compromise amounts.

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

Yes

The information (including identification, contact, financial, personal, and employment information) collected 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 borrowers and grantees.

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

The information is obtained from the borrowers, co-borrowers, co-signers, references provided by the borrowers, educational institutions, financial institutions, employers, the Department, the FSA National Student Loan Data System (NSLDS), National Student Clearinghouse (NSC), and external databases (e.g., Directory Assistance, credit bureaus,

skip-trace vendors, commercial person locator services, and the U.S. Department of the Treasury (Treasury)).

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

The information is collected via the following channels:

- Phone calls, emails, and web chats with customer service agents.
- Entries via the Interactive Voice Response (IVR) service.
- Incoming paper correspondence (e.g., via U.S. mail).
- Borrowers' usage of the servicers' websites.
- Secure data transmission within FSA systems.
- Secure data transmission from the Treasury.

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?

PII is directly received from borrowers during the loan application process. PII is used to authenticate users during online account creation for access to servicer portals and telephone calls. If a borrower 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 changes provided by FSA systems, skip tracing, Directory Assistance, National Change of Address Database (maintained by the U.S. Postal Service (USPS)) and other third parties (e.g., educational institutions, financial institutions, loan services and consumer reporting agencies, and Federal agencies (e.g., Treasury)).

Use

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

The information is collected to complete official Department business related to the servicing of loans. The information is necessary to uniquely identify individuals and to service their student loans on behalf of FSA. Servicers use this information to store, retrieve, and manage loan payments and loan balances. This information may be collected as part of the student loan application, processing, collection, and disposition of the borrower's account. This information is also used for individuals to electronically sign forms associated with management of their loan payment programs.

[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.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the 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.

3.8. 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

The SSN is the unique identifier for Title IV programs and its use is required by program participants and trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. Trading partners include the Internal Revenue Service (IRS), educational institutions, financial institutions, loan services, and consumer reporting agencies. The SSN is used for the following functions:

- To determine eligibility of individuals to receive a benefit on a loan (such as deferment, forbearance, discharge, or forgiveness).
- As a unique identifier in connection with the exchange of information between servicers and its trading partners (e.g., educational institutions, financial institutions, loan services, and consumer reporting agencies) that is performed in association with the servicing of the loans.
- As a data component for submission of loan data to NSLDS and Tax Form 1098-E data to the IRS.

- To locate an individual and to report and collect on the loans in case of delinquency or default.

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

☐ N/A

Alternatives to using SSNs have been considered but were determined to not be feasible given the design of systems at FSA and other Federal agencies, as well as the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA's data exchanges rely on SSN and date of birth to identify and track aid recipient's loans, grants, and payments.

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.

A Privacy Act Statement is located on the Free Application for Federal Student Aid (FAFSA) form and there is a link to the privacy policy on the FAFSA online application website for information that is collected by the Department.

For servicers acting on the behalf of the Department, there are privacy policies located within each respective servicer's website. In order to establish an online account with specific servicers, the borrower must agree to the "Terms of Service," which incorporate the privacy policy by reference and link. In addition, servicers will send a written privacy notice to borrowers when they initially turn over the loans for debt collections to the DMCS and annually thereafter.

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

A privacy notice is presented to the borrower via the following channels:

- FAFSA Application: Free Application for Federal Student Aid (FAFSA) form and there is a link on the FAFSA online application website to the privacy policy. (https://studentaid.ed.gov/sa/privacy)

- Servicers: To view the privacy notices 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.

4.3. 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 borrower has the opportunity to decline to provide the information; however, providing certain information is required in order to (i) communicate with websites or customer service call centers, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness). Servicers use the information only to process and service the borrower's loans as permitted by the Higher Education Act.

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

Information is shared with the Department's Office of the Inspector General (OIG) for fraud investigations.

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

☐ N/A

In the event of a fraud investigation, PII can be shared with the Department's OIG.

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

Servicers may share information with the following external entities:

- Educational institutions to coordinate the management of the loan with the educational institution's financial office.
- Credit bureaus to update loan payment status.
- Skip tracing vendors to locate individuals.
- Person locator services to obtain updated contact information.
- Other third parties as authorized by the borrower (e.g., employers, references).
- USPS for directory assistance, and the national change of address database to obtain forwarding addresses.
- Treasury for payment processing, collection of IRS refunds, and revisions for borrower PII updates.
- Other government entities (e.g., State attorney(s) general, Consumer Financial Protection Bureau (CFPB)) for reporting purposes.
- Digital signature vendors to assist in the signature process for official documents.

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

☐ N/A

The information is shared for the following reasons: to uniquely identify individuals; to determine program eligibility and benefits; to facilitate default reduction efforts by program participants; to enforce the conditions or terms of a loan or grant; to make, service, collect, assign, adjust, transfer, refer, or discharge a loan; to counsel a debtor in repayment efforts; to investigate possible fraud or abuse; to verify compliance with program regulations; to locate a delinquent or defaulted borrower; to prepare a debt for litigation; to prepare for, conduct, or enforce a limitation, suspension, termination, or debarment action; to ensure that program requirements are met; to verify whether a debt

[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.

qualifies for discharge, cancellation, or forgiveness; to conduct credit checks; to investigation complaints, update information, or correct errors contained in Department records; to refund credit balances; and to report to state attorney general(s), CFPB as required. In addition, information is reported to the IRS as required by U.S.C. 6050P and 6050S.

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

The servicers maintain an internal record of each disclosure of PII made during the course of business operations.

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

☐ N/A

PII is shared externally 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.

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

Yes

The Department entered into a MOU with Treasury for loan payment processing. Commercial servicers procured by the servicer have entered into contracts that contain clauses to protect and safeguard Department data. The only entity where there is not an agreement in place is the USPS. Information requests made to the USPS are seeking publicly available information for forwarding addresses.

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?

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, borrowers may access their own information via a website at the following locations:

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

6.2. What procedures are in place to allow the subject individual to correct 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, borrowers may access their own information to correct any inaccurate or erroneous records via https://studentaid.gov/manage-loans/default and/or https://myeddebt.ed.gov.

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

This PIA, as well as the system of records notice listed in question 2.2, 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 CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authorization 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?

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 Authorization to Operate (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.

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.

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.

Servicers' security and privacy controls are monitored and tested on a regular basis. Servicers' ongoing activities include, but are not limited to, the following:

- Security and privacy documentation are updated annually
- Vulnerability scanning and penetration testing are conducted on a regular basis
- Plans of actions and milestones are created for all vulnerabilities identified
- Training is conducted at least annually
- An ATO is obtained every three years
- All major system changes must go through a rigorous configuration management process that includes testing for any security and privacy impacts
- Quarterly security and privacy forums are held by the Department
- Continuous monitoring through the Department's Cybersecurity Framework Risk Scorecard provides the system owner and necessary stakeholders with a detailed view of the system's implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and associated risk level.

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 that the privacy risks are properly assessed, by ensuring Privacy Act records are maintained in accordance with the provisions of the Privacy Act and the published system of records notice, by ensuring appropriate security and privacy controls are implemented to restrict access, and by properly managing and safeguarding PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the Information System Security Officer (ISSO), and participates in FSA's life-cycle management methodology, which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews interfaces between FSA systems, as well as systems of records notices that govern data maintenance and use.

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 associated with servicers include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII 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 granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission. Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. As referenced above, patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.