Privacy Impact Assessment (PIA)

for the

Debt Management and Collection System (DMCS)

December 22, 2021

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Diana O'Hara** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Diana O'Hara
Contact Email: Diana.O'Hara@ed.gov

System Owner

Name/Title: Shital Shah
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.

The Debt Management and Collection System (DMCS) is a Federal Student Aid (FSA) system that supports the transfer of loans that are in default from FSA servicers in order to assist in the collection of those loans. DMCS works with defaulted borrowers to facilitate repayment of loans through potential income-contingent[1] repayment or forbearance[2] options. Payments on defaulted borrower accounts are processed through the U.S. Department of the Treasury's (Treasury) National Payment Center (NPC). FSA communicates with borrowers through U.S. mail, email, or phone calls in order to inform the borrowers of wage garnishment actions, selections of income-contingent repayment options, and changes in repayment status. Other functions of DMCS include loan collection activities, working with the U.S. Department of Justice and the Treasury on garnishment, and recovering loan balances through Internal Revenue Service (IRS) refunds. Throughout the process, information is provided to credit bureaus concerning the status of defaulted loans. DMCS maintains not only loan information, but borrowers' personally identifiable information (PII) to support payment and collections processing and reporting of loan statuses to other FSA systems.

The DMCS system is comprised of two websites: Myeddebt.ed.gov (the front-end public site for borrowers' debt resolution), and an internal site (for back-end DMCS business operations staff). DMCS uses mid-range platforms and back-end databases to support the servicing of defaulted loans, processing loan payments, and reporting on loan information.

1.2. Describe the purpose for which the personally identifiable information (PII)[3] is collected, used, maintained, or shared.

PII is collected to identify individual debtors and to complete official government business related to the collection of student loan debt. DMCS requires PII to perform loan processing and debt collection support for debts in accounts for the U.S.

[1] Income-contingent repayment bases borrowers' monthly payments on their incomes and family size.
[2] With forbearance, borrowers will not have to make a payment, or they can temporarily make a smaller payment for a specific timeframe.
[3] 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

Department of Education (Department).

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

The previous PIA expired. A review of the system determined the PIA should be updated to accurately represent the PII collected by the system.

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

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), Public Law 89-329, as amended, Section 441 and 461 Title IV, Section 401.

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 payment processing or responses to borrowers, loan information is retrieved using the borrower 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)).[4] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

□ N/A

DMCS is covered under the "Common Services for Borrowers" System of Records Notice (CSB SORN). The CSB SORN (18-11-16) was last published in the Federal Register at 81 FR 60683 (September 2, 2016). https://www.federalregister.gov/documents/2016/09/02/2016-21218/privacy-act-of-1974-system-of-records

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.

The DMCS 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

[4] 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

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.

DMCS receives and maintains the following information on borrowers that default on student loans:

- Full name
- Social Security number
- Driver's license or state identification (ID) number
- Date of birth
- Street address
- Telephone number
- Email addresses
- Employment information
- Borrower information (disbursement amount, principal balance, interest accrual, loan status, repayment amount, forbearance status, deferment status, separation date, grace period, and delinquency)

  Note: this PII is received from other FSA systems (e.g., loan servicers); however other information is provided by borrowers or payment information by the Treasury to maintain accuracy of the records.

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

Yes

The system collects PII to identify debtors, administer loans, and collect student loan debt. DMCS collects only that information required to accurately identify borrowers and to process loans and collect debts.

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

PII is collected directly from borrowers, from Title IV Servicers or the Department's National Student Loan Database system (NSLDS) or external agencies, such as the Department of Treasury. Please see the PIA for NSLDS to understand the sources of PII in that system.

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

PII is received from the following sources :

- Secure data transmission from Title IV servicers, NSLDS and the Department of Treasury.
- Phone calls with customer service representatives within the default resolution group contact center.
- Incoming correspondence (e.g., U.S. mail).
- Myeddebt.ed.gov website; borrowers can provide updates to currently maintained information (e.g., mailing address).

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[5] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

PII is received from other FSA systems (e.g., servicers); however other information is provided by borrowers or by the Treasury to maintain accuracy of the records. PII is used to authenticate users during online account creation for access to Myeddebt.ed.gov and telephone calls through the default resolution group contact center. If a borrower notes the PII that FSA maintains about them is incorrect, records are updated within the system. Additionally, PII updates will occur because of changes provided by FSA systems and the 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 government business related to the administration of collections. DMCS provides a vehicle for the storage, retrieval, and editing of debtor information and uses this information to collect debt from defaulted accounts. This information may be collected as part of the student loan application, processing, collection, and disposition of the account.

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

No

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

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

☑ N/A

Click here to enter text.

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 the Title IV programs and its use is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. Trading partners include other Federal agencies, institutions of higher education, national credit bureaus, lenders, and servicers.

DMCS uses the SSN for the following functions:

- To verify, identify, and determine eligibility 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 DMCS and its trading partners (e.g., educational institutions, financial institutions, loan servicers 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 the borrower 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

The SSN is a unique personal identifier. Alternatives were not considered based on the direct personal correlation between an individual and their SSN. The SSN offers the best option for identification, since it is the only common identifier that is used by the Department and its partners.

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 link to the privacy policy on the DMCS home page. The privacy policy can be accessed on the borrower's web portal and provided and stated during phone conversations.

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 privacy policy can be found at: https://myeddebt.ed.gov/borrower/#/privacy.

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?

During the student loan application process, individuals consent to their information being automatically transferred to DMCS upon defaulting on a loan. The individuals can decline to provide information and opt out of the student loan process or opt to fulfill the terms of their loans prior to their information being transferred from loan servicers. Through these opportunities, the borrower has the opportunity to decline to provide information to DMCS. However, providing certain information is required to (i) communicate with the DMCS system through its secure borrower portal website or custom call center, or (ii) receive certain benefits on a loan (such as deferments, forbearance, discharge, or forgiveness).

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 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.[6]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

□ N/A

DMCS will share information with the following external organizations for the purposes explained below:

- Treasury for payment processing, collection of IRS refunds, and revisions for borrower PII updates.

[6] 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.

- U.S. Department of Justice to issue wage garnishment orders.
- U.S. Department of Housing and Urban Development to support applications for low-income housing.
- Credit bureaus for reporting status of loans.
- United States Postal Service (USPS) for directory assistance, and the national change of address database to obtain forwarding addresses.

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

□ N/A

The information is shared with external entities to ensure data integrity and accuracy and for the purposes described above. The Department has entered into memoranda of understanding or information sharing agreement(s) with all of the entities listed above in Question 5.5 aside from the USPS. Information requests made to the USPS are seeking publicly available information in order to attain forwarding addresses for borrowers.

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

DMCS maintains an internal record of each disclosure of PII made during the course of its 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), MOU, or other type of approved sharing agreement with another agency?

□ N/A

Yes

The Department has entered into MOUs or ISAs with all the entities listed above in Question 5.5 aside from 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 location:

- https://studentaid.ed.gov/sa/repay-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.

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

The system of records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

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

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

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?

DMCS is maintained on secure computer servers located in one or more secure Department network server facilities. Access to DMCS is limited to authorized contractors and Department employees which include FSA employees, IT professionals working on DMCS, and contractor program managers who have responsibilities for DMCS and its hosting location. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, DMCS must receive a signed Authorization to Operate (ATO) from a designated Department authorizing official. Security and privacy controls implemented by DMCS are comprised of a combination of administrative, physical, and technical controls.

Physical access to the sites of the Department's contractors, where this system is maintained, is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge. All contract and Department personnel who have facility access and system access must undergo a security clearance investigation. Individuals requiring access to information subject to the Privacy Act of 1974, are required to hold, at a minimum, a moderate-risk security clearance level. These individuals are required to undergo periodic screening at five-year intervals. In addition to undergoing security clearances, contract and Department employees are required to complete security awareness training on an annual basis. Annual security and privacy training is required to ensure that contract and Department users are appropriately trained in safeguarding these data. The computer system employed by the Department offers a high degree of resistance to tampering and circumvention through the application of security controls. These controls limit data access to Department and contract staff 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 Department requires 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 information technology 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.

DMCS is scanned at least once per month by an independent third party to ensure the security controls in place are effectively securing data. DMCS also has a monthly patch management program, and vulnerability scans occur after the monthly patches have been implemented. Additionally, pre and post implementation scans are performed after monthly release activities to validate the release did not adversely affect the production environment. These scans are to validate that the implemented security controls continue to work properly. DMCS is required to submit plan of action and milestones (POA&Ms) quarterly, which continuously monitor any vulnerabilities and ensure any found vulnerabilities are mitigated and closed.

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 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 DMCS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of an administrative, technical, and physical controls to ensure that information is used in accordance with approved practices.

The second method is by ensuring that 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 address security and privacy risks through the system's lifecycle.

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 DMCS 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.