Privacy Impact Assessment (PIA)
for the

Debt Management and Collection System (DMCS)
November 4, 2019

For PIA Certification Updates Only: This PIA was reviewed on **November 4, 2019** 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: Federal Student Aid (FSA)

System Owner

Name/Title: Diana O'Hara
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 Collections System (DMCS) is the largest component of collections within Federal Student Aid. It provides a vehicle for the storage, retrieval, and editing of debtor information. Payments on defaulted accounts are processed through the National Payment Center (NPC) as part of this system. In addition, official correspondence to debtors from ED, the collection agencies, and other interested parties is provided by this system. Collection Agency Reporting, Treasury Offset, Administrative Wage Garnishment and Credit Bureau Reporting efforts are other parts of this system.

DMCS collects and maintains information considered to be Privacy Act Data (name, address, telephone numbers, e-mail addresses, employment information, SSN, etc.). This information is collected and maintained for borrowers that default on student loans.

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

The information is collected to complete official Government business related to the collection of student loan debt. DMCS requires PII data in order to perform loan processing and debt collection support for debts in accounts for the Department of Education nationwide. Without the PII data, DMCS cannot perform the responsibilities stated under the contract.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

[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

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

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

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), 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 or other identification?

Yes

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

☐ N/A

DMCS is covered under the "Common Services for Borrowers" System of Records Notice (SORN). The CSB SORN (18-11-16) was last published in the Federal Register at 81 FR 60683 (September 2, 2016).

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

https://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 and Maximus processes are under review for 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.

DMCS collects and maintains information for borrowers that default on student loans.

- Full name
- Social Security Number

- Driver's License or State 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)

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

Yes

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

PII is collected directly from borrowers, or obtained from Title IV Servicers (a complete list can be found as an attached appendix of the TIVAS/PCA PIA), or the Department's NSLDS 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 collected via:

- File transfer from the third party data providers as required,
- Secure data transmission from other Department of Education appliances (e.g., TIVAS servicers)
- Phone calls with Customer Service Representatives
- Incoming correspondence (e.g. U.S. mail)
- Borrower web portal

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?

The information is validated via identity verification and authentication during on-line account creation and telephone calls, verification between internal databases maintained in Department systems, and data exchange with external trading partner databases such as:

- Consumer reporting agencies
- Other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system
- United States Postal Service (USPS)

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 defaulted accounts. This information may be collected as part of the student loan application, processing, collection, and disposition of the account. This information is available through a DMCS Business Partner WEB Portal allowing ED and Private Collection Agencies access to the data.

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

Click here to enter text.

Social Security Numbers

[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.

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 the Department of Education, the Internal Revenue Service, 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, and 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 DoED 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.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

There is a Privacy Act Notice on the Debt Management Collection System (DMCS). The Privacy Act Notice can be found on the form, when accessing the system, and provided and stated during phone conversations. The PIA and SORN are also forms of notice.

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

https://myeddebt.ed.gov/DebtResolutionPrivacy.html

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?

Individuals have already provided the information contained in DMCS via the Federal student loan application process.

During the student loan application process individuals consent to their information being automatically transferred to DMCS upon defaulting on a loan. They 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 in order 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

The information shared is sensitive student level data as it pertains to students who have defaulted student loans. The Department may disclose information in this system without the consent of the individual, in accordance with the provisions of the Privacy Act of 1974.

- National Student Loan Data System (NSLDS)
- Financial Management System (FMS)
- Common Origination and Disbursement (COD)

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

☐ N/A

In accordance with requirements set forth by DoED, the DMCS shares information with DoED to allow it to administer the Direct Loan Program. The purpose of sharing the information in DMCS with the other FSA systems is to ensure accuracy of the borrower data.

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

[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.

whom and for what purpose.

☐ N/A

DMCS will share information with an external organization only if a Memorandum of Understanding (MOU) and Interconnection System Agreement (ISA) are established. There will be no sharing of information outside the purpose of collecting information and being compliant with the MOUs and ISAs.

ED-Contracted Partner Systems:

- Private Collection Agencies (PCAs)
- TIVAS (Title IV Additional Servicers)
- Perkins
- Nelnet
- Department of the Treasury and the Internal Revenue Service
- Department of Housing and Urban Development
- Credit Reporting Agencies
- Consumer Reporting Agencies
- Collection Agencies
- National Payment Center
- United States Postal Service, Directory Assistance, National Change of Address Database

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

☐ N/A

The purpose of sharing information with specific external organizations is to ensure data integrity and accuracy. There will be no sharing of information outside the purpose of collecting information and being compliant with the MOUs and ISAs.

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

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

☐ N/A

The data is transferred through secure file transfer protocol (sftp) or through FSA's Student Aid Internet Gateway.

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

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?

Procedures for allowing individuals to access their own information are explained in the System of Records notice listed in question 2.2. 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?

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

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

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

7. Safeguards

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

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

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

High

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

In accordance with the Federal Information Security Management Act of 2002 (FISMA), DMCS must receive a signed Authority To Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones (PO&AMs) to remediate any identified deficiencies, and a continuous monitoring program. FISMA controls implemented by DMCS are comprised of a combination of management, operational and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environment protection, planning, personnel security, risk assessment, system and service acquisition, system and communications protection, system and information integrity, and program management. The Department will follow all Federal laws, standards and guidelines and Department of Education polices DMCS must comply with.

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 DMCS production environment is scanned at least once per month by a third party to ensure the controls in place are effectively securing our 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 Plans of Actions and Milestones 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 of Education risk management framework process in order to receive an Authority to Operate (ATO). During the ATO process DMCS makes sure that the National Institute of Standards and Technology (NIST) 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 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. Borrowers are assigned an ID that is not based on their SSN. 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.