Privacy Impact Assessment

For
Debt Management and Collection System (DMCS)

Date:
June 30, 2014

Point of Contact:

Consuelo Johnson

Consuelo.Johnson@ed.gov

System Owner:

Keith Wilson

Keith.Wilson@ed.gov

Author:

William Floria

WilliamEFloria@maximus.com

Office of Federal Student Aid (FSA)

U.S. Department of Education

1. System Information.

Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

Information System Name: Debt Management and Collection System

System Acronym: DMCS

Operator of the System (on behalf of Federal Student Aid): MAXIMUS Federal Services

The Debt Management and Collection 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, Social Security Number, etc.). This information is collected and maintained for borrowers that default on student loans.

2. Legal Authority.

Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The Higher Education Act of 1965 (HEA), As Amended, Section 441 and 461 Title IV, Section 401.

3. Characterization of the Information.

What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

DMCS collects and maintains information for borrowers that default on student loans. The information is considered to be Privacy Act Data:

- Full Name
- Social Security Number (SSN)
- Home Address
- Telephone Numbers
- Email Address
- Employment Information
- Borrower Information (disbursement amount, principal balance, interest accrual, loan status, repayment plan, repayment amount, forbearance status, deferment status, separation date, grace period and delinquency)

The sources for the information are as follows:

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

The information is collected to complete official Government business related to the collection of defaulted student loan debt. Information is sent to the NSLDS system, which cross-references student loans from multiple databases.

4. Why is the information collected?

How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The information is collected to complete official Government business related to the collection of defaulted student loan debt.

The privacy risks related to storing the information within the system include among other things loss or confidentiality (inadvertent PII disclosure), integrity (incorrect data) and/or availability (system downtime) of the information within the system. Maximus Federal is aware of the risks associated with collecting and storing the personal information related to the student loan accounts. Successful security assessments and authorization are requirements for the system to operate. See question 11 for specific security and privacy controls.

5. Social Security Number (SSN).

If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The SSN is the unique identifier for 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, Internal Revenue Service (IRS), institutions of higher education, national credit bureaus, lenders and servicers.

DMCS2 uses the SSN for the following functions:

- To verify identity 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 the DMSC 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 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.

6. Uses of the Information.

What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

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

The information is collected to complete official Government business related to the administration of collections.

7. Internal Sharing and Disclosure.

With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

The borrower's personal information is shared for collection purposes with Federal Student Aid (FSA).

In accordance with requirements set forth by DoED, the DMCS share information with DoED to allow it to administer the Direct Loan Program. DoED my disclose information contained in a record in an individual's account in accordance with the Privacy Act 1974.

DMCS shares information with:

- Federal Student and its agents or contractors
- National Student Loan Data System (NSLDS)
- Common Origination and Disbursement System (COD)
- Student Aid Internet Gateway (SAIG)

Please refer to question 4, which describes what information is shared, for what purpose the information is shared, the risks to privacy for internal sharing and disclosure and how the risks are mitigated.

8. External Sharing and Disclosure.

With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

DMCS will share information with an external organization only if a Memorandum of Understanding (MOU) and Trading Partners Agreement (TPA) under OMB Circular A-130, Appendix III has been

completed. There will be no sharing of information outside the purpose of collecting information and being compliant with the MOUs and TPAs.

DMCS shares data with the following external entities:

ED-Contracted Partner Systems:

- Private Collection Agencies (PCAs)
- Guaranty Agencies (GAs) – Assignments, Recalls
- TIVAS (Title IV Additional Servicers) - Assignments, Recalls, Rehabs,
- Perkins – Rehabs, Non-Default
- TOP (Treasury Offset Program) – GA's
- FSA (Federal Student Aid) – FMS (Financial Management System)
- Common Origination and Disbursement (COD) – Pell Grants
- Total Permanent Disability (TPD) - Nelnet
- Post Secondary Education Participants System (PEPS) – School File
- Education Credit Management Corporation (ECMC) – Bankruptcy
- National Student Loan Data System (NSLDS)
- Direct Loan Consolidation System (DLCS) – Loan Verification Certificate (LVC) File

Other Government Partners:

- Treasury Lockbox - Bank of America
- Treasury - Pay.Gov
- Treasury – Treasury Offset Program (TOP)
- Internal Revenue Service (IRS) – Skip Trace, 1098/1099 Annual Reporting
- Housing and Urban development (HUD) – Credit Alert Interactive Voice Response System (CAIVRS)
- Health and Human Services (HHS) – New Data New Hire (NDNH)
- Department of Justice (DOJ)
- Social Security Administration (SSA)
- United States Postal Service (USPS) – Address Corrections

Other Non-Government Partners:

- Credit Bureaus – Reporting

9. Notice.

Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

There is a Privacy Act Notice on the DMCS website. It states the following:

Disclosure Statement:

"The Privacy Act of 1974 (5 U.S.C. 552a) requires that the following notice be provided to you:

The authority for collecting the requested information from and about you is 451 et seq. of the Higher Education Act of 1965, as amended (20 U.S.C. 1087a et seq.). The principal purpose for collecting information about you is to allow collection of defaulted federal education debt. Your disclosure of the requested information is voluntary, but you must provide the requested information in order to use the U.S. Department of Education's Debt Resolution Web site.

The information in your file may be disclosed to third parties as authorized under routine uses in systems of records notices #18-11-05, called Title IV Program Files, and #18-11-06, called National Student Loan Data System (NSLDS). The published routine uses of this information include its disclosure to federal, state, or local agencies, to other federal agencies under computer matching programs, to private parties such as relatives, present and former employers, business and personal associates, to credit bureau organizations, to educational institutions, and to contractors in order to verify your identity, to determine your Program eligibility and benefits, to permit the servicing or collection of your loan(s), to counsel you in repayment efforts, to enforce the terms of the loan, to investigate possible fraud and to verify compliance with Program regulations, or to locate you if you become delinquent in your loan(s) payments or you default. In the event of litigation, we may send records to the Department of Justice, a court, adjudicative body, counsel, party, or witness if the disclosure is relevant and necessary to the litigation. If this information, either alone or with other information, indicates a potential violation of law, we may send it to the appropriate authority for action. We may send information to members of Congress if you ask them to help you with federal student aid questions. In circumstances involving employment complaints, grievances, or disciplinary actions, we may disclose relevant records to adjudicate or investigate the issues. If provided for by a collective bargaining agreement, we may disclose records to a labor organization recognized under 5 U.S.C. Chapter 71. Disclosures may also be made to qualified researchers under Privacy Act safeguards. These published System of Records notices are located at http://www2.ed.gov/notices/sorn/18-11-05c_122799.pdf and http://www.gpo.gov/fdsys/pkg/FR-2011-06-24/pdf/2011-15747.pdf.

10. Web Addresses.

List the web addresses (known or planned) that have a Privacy Notice.

https://www.myeddebt.com/DebtResolutionPrivacy.html

http://www2.ed.gov/offices/OSFAP/DCS/index.html

11. Security.

What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

In accordance with the Federal Information Security Management Act of 2002 (FISMA), every FSA system 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 actions and milestones to remediate any identified deficiencies, and a continuous monitoring program DMCS received its ATO on June 2014.

FIMSA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Additionally, the following specific controls are applied:

Management Controls

- Security Assessment and Authorization
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational Controls

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environment Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical Controls

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)

- System and Communications Protection (SC)

Privacy Controls

- Authority and Purpose (AP)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

DMCS employs administrative, technical and physical security controls of its facilities and systems in accordance with the Federal Information Security Management Act (FISMA). PII is protected following the guidance of OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, Computer Security Act of 1978.

Access Control

A formal documented Access Control Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities and compliance along with formal , documented procedures to facilitate the implementation of the Access Control Policy and associated access controls, is disseminated and periodically reviewed and updated when necessary. Proper identification is required to establish system access, and access is granted based on a valid access authorization and intended system usage. All users are assigned a unique identifier. All unnecessary accounts are removed, disabled or otherwise secured. Inactive user accounts are disabled automatically. The concept of least privilege is employed, allowing only authorized access and privileges for users (and processing acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with agency missions and business functions. System access is authenticated with strong passwords and multi-factor authentication.

Audit and Accountability

Event logs from authentication sources, network devices and security technologies are centrally captured and contain sufficient information to establish the types of event, the date and time the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. The vent logs are secured from unauthorized viewing, modification and deletion.

System and Communication Protection

Boundary protection measures are employed to safeguard the DMCS system and control information flow between information systems. All Internet traffic originating from within the DMCS system is controlled through proxies and content filters. Firewalls are deployed at the Internet boundary.

The confidentiality and integrity of information transmitted between the DMCS system and other external systems is protected by cryptographic mechanisms. Inbound and outbound DMCS traffic is inspected using an industry standard intrusion protection system. All portable media, such as paper, backup tapes and CDs, are encrypted to otherwise physically secured, and accountability for the portable media during transport is maintained.

The DMCS system servers and workstations have malicious code protection installed and operational. Incoming electronic mail is canned for span and viruses and is cleansed or quarantined when necessary.

Personnel Security

Employees receive annual security awareness training and are specifically instructed on their responsibility to protect the confidentiality of PII. All DMCS systems users with access to PII are required to submit to a security background check and to obtain at least a 5C security clearance.

Physical Security

Physical access to the facility is controlled through the use of proximity cards. Employees wear identification badges. All visitors who access non-public areas must provide photo identification, and each person's access is recorded. Visitors requiring an escort are given red "escort required" badges which must be worn at all times in the facility. The physical security of the facility is monitored 24 hours a day, 7 days a week by a monitoring company. Video surveillance from cameras is captured and digitally recorded 24/7.

The DMCS system is compliant with the following Federal Standards and Guidelines:

- Federal Information Security Management Act (FISMA)
- Privacy Act of 1974
- E-Government Act of 2002
- Federal Information Security Controls Audit Manual (FISCAM)
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
- NIST SP 800-35, Guide to Information Technology Security Services, October 2003
- NIST SP 800-37, Rev. 3, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- NIST SP 800-40, Procedures for Handling Security Patches, November 2005
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-42, Guidelines on Network Security Testing, October 2003
- NIST SP 800-44, Rev. 2, Guidelines on Security Public Web Servers, September 2007
- NIST SP 800-45, Rev. 2, Guidelines on Electronic Mail Security, February 2007
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002

- NIST SP 800-50, Building an Information Technology Security Awareness Program, October 2003
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-55, Rev. 1, Performance Measurements Guide for Information Security, July 2008
- NIST SP 800-58, Security Considerations for Voice Over IP Systems, January 2005
- NIST SP 800-60, Rev. 1, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-60, Rev. 1, Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-61, Rev. 1, Computer Security Incident Handling Guide, March 2008
- NIST SP 800-64 Rev. 2, Security Considerations in the Systems Development Life Cycle, October 2008
- NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process. January 2005
- NIST SP 800-70, Rev. 2, National Checklist Program for IT Products: Guidelines for Checklists Users and Developers, February 2011
- NIST SP 800-77, Guide to IPsec VPNs, December 2005
- NIST SP 800-81, Rev. 1, Secure Domain Name System (DNS) Deployment Guide, April 2010
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005
- NIST SP 800-88, Guidelines for Media Sanitization, September 2006
- NIST SP 800-92, Guide to Computer Security Log Management, September 2006
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- NIST SP 800-95, Guide to Secure Web Services, August 2007
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
- NIST SP 800-113, Guide to SSL VPNs, July 2008
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, April 2010
- NIST SP 800-123, Guide to General Server Security, July 2008
- NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008

12. Privacy Act System of Records.

Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

DMCS is 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 January 23, 2006 (71 FR 3503-3507).

13. Records Retention and Disposition.

Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

DMCS follows the "Loan Servicing, Consolidation, and Collections Records".

ACS Tracking Number: OM: 6-106:L47

Schedule Locator NO: 075

Draft Date: 1/28/2010

Title: FSA Loan Servicing, Consolidation, and Collections Records

NARA Disposition Authority: N1-441-09-16