# Privacy Impact Assessment (PIA)
for the

Customer Engagement Management System (CEMS)

Dec 24, 2018

This PIA was originally approved on Oct 22, 2018 and reviewed on Dec 3, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: ShaVon Holland, ISSO

Contact Email: Shavon.holland@ed.gov

System Owner

Name/Title: Joyce Demoss, Ombudsman

Program Office: Federal Student Aid (FSA)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.***

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

Customer Engagement Management System (CEMS) integrates multiple customer-engagement services in FSA into a singular customer-relationship management (CRM) platform; controlling costs, delivering multi-media contacts, and person-to-business channel support. The Department of Education, FSA, possessed the need to acquire a CRM systems support solution to enable varied FSA business operations to co-exist in a shared contact and information sharing solution for customer management efficiencies, costs control, and detailed customer-engagement activities to resolve customer issues, or to inform ongoing business decisions concerning FSA products, services, and where needed, to inform on existing, or in-progress education policies/decisions. CEMS currently encompasses the Feedback Dispute Management System (FDMS) and Borrower Defense application. In FY2016, FSA embarked on meeting this need through the acquisition of software as a service (SaaS) solution to meet the need, but not incur the costs associated with an on-site underlying production (hardware/centers) environment. The acquisition activity led to the implementing of the Salesforce/SaaS with Community of Practice Service Module. Software as a Service (SaaS) includes the enabling design/development products, services, support licensing, operations and maintenance (O&M) as inclusive services in the delivery model. The finished delivered platform product (CEMS) was designed and enabled to meet the FSA requirements need. The delivered CEMS also includes training support on the use of the products/services to meet ongoing, continuous customer-engagement activities, both internally and externally managed and operated, as needed.

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

Information is used to establish contact with the customer seeking our assistance (multiple contact means are desired), as well as to establish contact means to individual(s) relevant to finding resolution on a customer/ borrower's student aid issue(s), feedback or compliment. Additionally, the customer's DOB and SSN are required to match other financial and disbursement databases to establish the financial aid history, accuracy and facts associated with the customer's claims. Summarized text entries of conversation facts detail the contact history, and eventual outcome to the customer/borrower's student aid issue(s).

The FDMS has been classified as Mission Important, Low Risk of inflicting grave harm either upon an individual or the Department of Education if internal data should be compromised. The Ombudsman Group is responsible for routine monitoring of the operation of the CEMS to ensure sound practices are being observed by staff to protect Privacy Act data and the various forms of access to the CEMS.

[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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

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? If this is an update, please include the publication date of the original.

New PIA

Original Publication Date:

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

Contractor

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?

The Student Loan Ombudsman is mandated by Congress in the Higher Education Act, as amended, 20 USC 1018.SEC.141 (f). The Student Loan Ombudsman provides timely assistance to borrowers of loans made, insured, or guaranteed under Title IV. The Feedback and Dispute Management System (FDMS) is the primary information technology resource used by the Ombudsman Group to meet the directed mandates of Congress to assist borrowers, track issues and complaints, and document and report on activities.
On March 10, 2015, President Obama continued his vision for affordable quality education for all Americans through the creation of a Student Aid Bill of Rights (SABR). The Memorandum included the creation of a state-of-the art complaints system to ensure quality, service, and accountability for the DoED, its contractors, colleges, and loan servicers. This is now known as FDMS.
Under the Higher Education Act (Sec.455(h)), a student loan may be forgiven under certain circumstances: borrower's death or disability, closure of the school the borrower attends; public service overtime; false certification by the institution of the borrower's eligibility for federal student aid; and certain institutional misconduct harmful to the student. The last of these is referred to as a borrower defense. FSA determined a need to review the existing and future requirements to support borrower defense across technology, contractors and operations. It was determined to leverage the CEMS platform for the borrower defense application. The application will support the review processes for borrower defense.

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? Please answer **YES** or **NO**.

Yes

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

Customer Engagement Management System (CEMS) (18-11-11) published in the Federal register on June 13, 2018, 83 FR 27587.

https://www.federalregister.gov/documents/2018/06/13/2018-12700/privacy-act-of-1974-system-of-records

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 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

There is a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development life cycle and for the data collected at Schedule Locator No. 052: Ombudsman Case Files. NARA Disposition Authority N1-441-09-21.

ED 052 is being amended, pending approval by NARA. Records will not be destroyed until NARA-approved amendments to ED 052 are in effect, as applicable.

[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

2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

3.1 List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

The following data is collected and maintained in CEMS:

Name (First, Middle, Last)
Date of Birth (DOB)
Social Security Number
Current Address
Current Telephone Numbers (e.g. Work, Home, Mobile)
Email Address
Facsimile Number
Written summary of the student aid issue(s)/complaint(s)/compliment(s) that brought the customer/borrower to FSA seeking resolution assistance
Written summary of all relevant information obtained to research and resolve the customer's issue(s)/complaint(s)/compliment(s)

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

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

The sources of information include individuals such as the complainant or primary contact. The primary contact is not just limited to the complaint. The primary contact could be any approved third party authorized to act on the complainant's behalf such as an attorney, relative, representative, friend, etc. Schools and external/internal agencies and various organizations provide information in CEMS as well.

3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

CEMS receives customer requests for assistance, complaints and compliments via the customer portal, phone, email, postal mail and facsimile. These requests are generally from recipients of Title IV Aid. CEMS does not generally receive requests from teachers, employees or universities.

3.5 How is this information validated or confirmed?[3]

Customers interacting with the FDMS Customer Portal can choose to authenticate or not authenticate when submitting compliments, complaints, and reports of suspicious activity to FSA. More specifically, customers have the following options:
1. Log in with their FSA ID and password (Authenticated Customer)
2. Continue without an FSA ID (Unauthenticated-Identified Customer)
3. File anonymously (Unauthenticated-Anonymous Customer) – this option allows customers to maintain confidentiality when submitting sensitive information or reporting wrongdoing.

If the customer chooses to provide their FSA ID and password, they will be redirected to the FSA ID website to log in. If the customer chooses to proceed without an FSA ID or file anonymously, they will proceed directly to the next step in the submission process. Authenticated users, once logged in, will have the additional ability to view and update their existing FDMS cases, as well as initiate live chat support sessions with Contact Center personnel. Unauthenticated-Identified and Unauthenticated-Anonymous Customers are not able to update and track their case submissions and cannot initiate live chat support sessions, but may still request a response to the contact email/phone they provide. Information is validated by PAS/FSA ID and through communication with the customer and reference of other databases such as NSLDS, COD, etc.

[3] Examples include form filling, account verification, etc.

Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

Information is used to establish contact with customer seeking our assistance (multiple contact means are desired), as well as to establish contact means to individual(s) relevant to finding resolution on a customer/borrower’s student aid issue(s). Additionally, summarized text entries of conversation facts detail the contact history and eventual outcome to the customer/borrower’s student aid issue(s), complaints and compliments.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

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

3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 ☒ N/A If the above answer is **YES,** please explain.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.9 Does the system collect Social Security Numbers? Please answer **YES** or **NO**.

Yes

3.9.1 □ N/A If the above answer is **YES,** explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

The customer's DOB and SSN are required to match to other financial and disbursement databases to establish the financial aid history accuracy and facts associated with the customer's claims.

No other alternatives are used in place of the SSN, as this information is requested to research customer requests for assistance, complaints and compliments.

3.10 □ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

SSN is a universal way of identifying individuals. In addition to the SSN, we also collect FSA IDs but when not available, the SSN must be used to create an unique identifier.

4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

A privacy policy and Privacy Act information is posted on the studentaid.ed.gov website that provides notice to customers regarding the purpose for which their data is collected, how it is used, to whom it is disclosed, how it is protected, and other privacy information. All information provided to address the customer/borrower’s student aid issue(s), complaints and compliments is provided voluntarily. At any point, individuals can decline to provide information.

4.2 □ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

Customer Engagement Management System:
https://fsaocts.my.salesforce.com/

Customer Engagement Management System Partner Portal:
https://feedback.edpartner.ed.gov

Coalition of Federal Ombudsman:
https://federalombuds.ed.gov

StudentAid.gov
https://studentaid.ed.gov/sa/privacy

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals submitting feedback through the system are encouraged to log in with their FSAID which links the system to their PII and student loan history. The language below is provided to individuals before completing a case.

"You may submit feedback without logging in; however, most cases require ED to review your federal student aid history and it may take longer for us to research your case. We recommend logging in with your FSA ID so that we can review your federal student aid history and determine next steps as quickly as possible. If you do not want to log in with your FSA ID, you may still choose to submit feedback and share your contact information with us so we can communicate with you. If you choose not to share any of your information, you will not hear back from ED, we will not be able to communicate with you to gather more information, and your case will be used for our records."

If individuals decline to provide information, FSA may not be able to research the customer's complaint or provide a response regarding the complaint. Individuals can opt out of the project before submitting a case by exiting the project. If a case has been submitted, they can request a case closure via email, mail, facsimile or telephone.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2 □ N/A What information will be shared and with whom?

Information about customer inquiries is compiled into CEMS. The data is analyzed, and the findings are included in internal reports for FSA, to identify systemic issues affecting Title IV programs.

5.3 □ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The data is analyzed, and the findings are included in internal reports for FSA and the industry in general, to identify systemic issues affecting Title IV programs.

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

Yes

5.5 □ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

To date, borrower/customer identification information has been shared with the Social Security Administration, the Internal Revenue Service, the Department of the Treasury, and the Consumer Financial Protection Bureau. In addition, information may be shared with Schools, Financial Institutions, Servicers, Lenders and State accrediting and guaranty agencies.

The Department may also disclose information under routine uses found in the SORN on a case by case basis.

5.6 □ N/A What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

Federal agencies, State agencies, accreditors, schools, lenders, guaranty agencies, servicers, and private collection agencies" when further information is necessary to the resolution of the request.

When sharing information with external entities, the Department's security standards that relate to protection of PII is followed.

5.7 □ N/A How is the information shared and used by the external entity?

Information is shared with Federal agencies, State agencies, accreditors, schools, lenders, guaranty agencies, servicers, and private collection agencies" when further information is necessary to the resolution of the request.

When sharing information with external entities, the Department's security standards that relate to protection of PII is followed.

5.8 □ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

No

5.9 □ N/A Does the project place limitation on re-disclosure? Please answer **YES** or **NO**.

Yes

6. Redress[4]

6.1 What are the procedures that allow individuals to access their own information?

Individuals are able to log into the system to access and review their own information. Individuals can also access their information through a Privacy Act request or by contacting the system manager and following the procedures listed in the SORN.

https://www.federalregister.gov/documents/2018/06/13/2018-12700/privacy-act-of-1974-system-of-records

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

6.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Inaccurate and erroneous information regarding contact and case detail information can be corrected by logging into FSAID and updating their information through that site. Information can also be updated by placing a request via email, telephone, facsimile, or mail.

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

CEMS users are unable to update customer information if they are authenticated users. Authenticated customers are advised either verbally or by written communication (letter or e-mail) that they must login to the FSA ID site to update their information.

Unauthenticated users can request their information be updated by contacting their case worker of the toll-free telephone line.

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? Please answer **YES** or **NO**.

Yes

7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

CEMS leverages enterprise data sharing rules that restrict visibility into data records. Each user within CEMS is set up with a profile and role, which dictates a user's level of access to objects as well as records, within those objects as defined by the data sharing rules.

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

Physical and environmental security controls have been implemented to protect the Salesforce facility housing system resources, the system resources themselves, and the facilities used to support their operation. The data center hosting provider employs and maintains fire detection and suppression systems throughout the data center. Fire detection systems include early smoke detection and smoke detectors. The fire suppression system includes dual-alarmed, dual-interlock, multi-zone and pre-action dry pipe water-based fire suppression.

Additional administrative, technical and physical safeguards in place include the following:

Technical and/or security evaluation
Risk Assessment
Rules of behavior established and signed by users
Contingency plan
Security plan
In-place security safeguards (monitoring, auditing, authentication and firewalls) and planned security safeguards (PIV-I use for system administrators)

7.4 Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

Yes

7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

FSA conducts a variety of security testing activities across the enterprise as part of an overall risk management and continuous monitoring strategy. Some of these activities are ongoing, including infrastructure scans and Ongoing Security Authorization assessment testing, and some are performed as needed for major system changes, including ad hoc scans, Production Readiness Reviews, Security Impact Analyses, and system self-assessments.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

The system owner receives notices from the ISSO of any atypical behavior by users. The ISSO and system owner receives a weekly security report which includes a list of active and inactive users, instances of atypical behavior.

In addition, the system ensues a Standards and Practices committee in which decisions are made regarding the business process for business units with users in the CEMS platform. That information is then diseminated to individual users based on their business units. Business units are also responsible for reporting any inappropriate behavior to the ISSO and System Owner so next steps can be determined.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

Since this is the first time using a SAS platform for the agency there is a high chance of performance issues. CEMS is used to collect and aggregate large amounts of Sensitive PII. Strict access controls, including two-factor authentication, and cyber security awareness training help to reduce the risk of intentional and unintentional releases of PII data.

To mitigate this risk CEMS employs the below procedures:

- conducts weekly operations meeting to ensure system functionality and discuss any problems, incidents or improvements for the system
- mitigates Plans of Actions and Milestones findings as soon as possible
- monitors atypical use of the system