



## Privacy Impact Assessment (PIA) for the

Digital Communications Tool

Nov 3, 2017

This PIA was approved on Nov 22, 2017 and reviewed on Nov 22, 2017 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:** Jessica Barrett Simpson, System Owner

**Program Office:** Federal Student Aid (FSA)

### Reviewing Official

**Kathleen Styles**

**Chief Privacy Officer**

**U.S. Department of Education**

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at [privacysafeguards@ed.gov](mailto: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  N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

The Digital Communications Tool (DCT) will enable Federal Student Aid (FSA) to improve communications for students, parents, and borrowers. The functionality includes the ability to do message testing, group customers, personalize communications, and track outcomes. It makes it easier for FSA staff to modify communications and do ad hoc campaigns when necessary, which will increase operational flexibility and efficiency. It will also allow FSA to add text messaging as a communications channel.

1.2  N/A Describe the purpose for which the personally identifiable information (PII)<sup>1</sup> is collected, used, maintained or shared.

DCT will have a system interface with the Central Processing System (CPS) and the Common Origination and Disbursement (COD) system.

The PII will include first name, email address and mobile number.

The purpose of the PII is to send customers emails and text messages about their FAFSA and student loans.

<sup>1</sup> 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  N/A Is this a new system, or one that is currently in operation?

New System

1.4  N/A 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  N/A 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  N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

The Higher Education Act of 1965 Amended.

## SORN

2.2  N/A 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**.

No

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)).<sup>2</sup> Please provide the SORN name and number, or indicate that a SORN is in progress.

### Records Management

*If you do not know your records schedule, please consult with your records liaison or send an email to [RMHelp@ed.gov](mailto:RMHelp@ed.gov).*

2.3  N/A 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.

Customer email and text messages are considered to be transitory, which is covered under GRS 5.2 - <https://www.archives.gov/files/records-mgmt/memos/grs5-2-initial-review-package.pdf>

<sup>2</sup> 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  N/A 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  N/A 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.

First name, email address, and mobile number.

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

The sources of information are the Central Processing System (CPS) and the Common Original and Disbursement System (COD).

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

Names, email addresses, and mobile numbers are collected online through FAFSA.gov and StudentLoans.gov. There are a limited number of FAFSAs submitted via paper form.

3.5  N/A How is this information validated or confirmed?<sup>3</sup>

The email addresses are validated using an automated process to confirm the email is entered correctly.

<sup>3</sup> Examples include form filling, account verification, etc.

**Use**

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

The system uses the information to send customers emails and text messages about their FAFSA and student loans.

3.7  N/A 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  N/A 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  N/A Does the system collect Social Security Numbers? Please answer **YES** or **NO**.

No

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.\*

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

#### 4. Notice

4.1  N/A 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 notice is provided to the user prior to the collection of their information. The Privacy Act provides the individual the ability to access their account and the right to request an amendment of any inaccurate information in their record. The individual may request the information in their record from ED by calling 1-800-4FED-AID (1-800-433-3243). A full explanation of the individual's rights under the Privacy Act is set forth in the Department's Privacy regulations.

CPS SORN: <https://www.gpo.gov/fdsys/pkg/FR-2011-08-03/pdf/2011-19607.pdf>

COD SORN: <https://www.gpo.gov/fdsys/pkg/FR-2010-09-27/pdf/2010-24162.pdf>

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

CPS Privacy Act Notice: <https://fafsa.ed.gov/privacynotice.htm>

COD Privacy Act Notice: <https://cod.ed.gov/cod/Privacy>

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

For most of the emails, customers cannot opt out because the emails are considered to be transactional, such as a confirmation email that a customer has submitted a FAFSA. The customer provides their email as part of the process and agrees to receive communication about their application. For non-transactional emails however, customers will be able to opt out by clicking on a link in the message or logging onto their online account.

## 5. Information Sharing

### Internal

5.1  N/A 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?

A limited number of FSA staff (fewer than 20) and Contractors (fewer than 20) will have access to the system for the purposes of setting up email and text messaging campaigns. However, most of those users will not have access to the person-level data. That will be limited to fewer people. Only four FSA staff will have the user level access to actually send emails and texts.

The system will be accessed through FSA's Access and Identity Management System (AIMS). AIMS uses two-factor authentication.

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 purpose of the data sharing is to set up and manage email and text messaging campaigns, which aligns with the stated purpose in Question 1.2.

**External**

5.4  N/A 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.

No

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.

5.6  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?

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

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**.

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

## 6. Redress<sup>4</sup>

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

Customers can access and/or update their information online at [StudentLoans.gov](http://StudentLoans.gov), [FAFSA.gov](http://FAFSA.gov), or [NSLDS.ed.gov](http://NSLDS.ed.gov).

<sup>4</sup> 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  N/A What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Customers can access and/or update their information online at StudentLoans.gov, FAFSA.gov, or NSLDS.ed.gov.

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

The email and text messages will include information about how to update their contact information and/or opt out of receiving messages as applicable.

## 7. Safeguards

*If you are unsure which safeguards will apply, please consult with your [ISSO](#).*

7.1  N/A 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  N/A 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?

The system will be accessed through FSA's Access and Identity Management System (AIMS). AIMS uses two-factor authentication. Users will be given access after filling out a form, agreeing to the rules of behavior, and providing evidence of cyber security training. The system has seven levels of user access. The system limits the number of users who are able to send emails and who are able to view customer-level data. The system also provides reports on when users access the system.

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

FSA is currently going through security reviews for the system and will follow standard FSA policies and procedures. FSA will minimize the amount of PII in the system, set up user permissions that limit access, and the system will be integrated with the Access and Identify Management System (AIMS). AIMS will provide an additional level of security.

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

Yes

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

Yes

7.6  N/A 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  N/A 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  N/A 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 is currently going through the Authority to Operate (ATO) security review for the system and will follow standard FSA policies and procedures.

## 8. Auditing and Accountability

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

The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology, which addresses security and privacy risks throughout the system's lifecycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of Records notices.

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

One privacy risk associated with the system is that emails and text messages could be sent to the wrong customer. This will be mitigated by a quality assurance monitoring process.