# Privacy Impact Assessment (PIA)

for the

# Digital Customer and Care (DCC)

# February 12, 2020

**For PIA Certification Updates Only:** This PIA was reviewed on **February 12, 2020** by **Theon Dam** certifying the information contained here is valid and up to date.

## Contact Point

**Contact Person/Title:** Theon Dam
**Contact Email:** Theon.S.Dam@ed.gov

## 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.

Digital and Customer Care (DCC) is a mission supportive, major application whose infrastructure is hosted on the FSA Cloud. The DCC platform is a unified digital front-end process to assist borrowers with all financial aid needs from origination and disbursement to repayment through a single consolidated website. The DCC major components are the Digital Platform, Marketing Platform, and Customer Care Platform.

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

Federal Student Aid (FSA) collects personally identifiable information on individuals throughout the student aid lifecycle for identity verification and financial aid eligibility. The DCC is the front-end process that connects the one, consolidated website for borrowers to interact with the various back-end systems that maintain and process the PII for multiple purposes throughout FSA. The PII collected via the DCC website will be transmitted, as appropriate, to National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), Central Processing System (CPS), and Customer Engagement Management System (CEMS). For more information on how your records are handled, please refer to those individual PIAs and SORNs at www.ed.gov/privacy.

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

New System

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

[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

New 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 authority to collect is based on the Higher Education Act (HEA) of 1965, as amended. Sections 483 and 484 of the Higher Education Act of 1965, as amended, gives FSA the authority to ask these questions, and to collect Social Security numbers (SSN), from both the applicant and their parents.

**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

[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

Federal Student Aid Application File (18-11-01). October 29, 2019. 84 FR 57856-57863. https://www.federalregister.gov/documents/2019/10/29/2019-23581/privacy-act-of-1974-system-of-records

Common Origination and Disbursement System (18-11-02). August 16, 2019. 84 FR 41979-41987. https://www.federalregister.gov/documents/2019/08/16/2019-17615/privacy-act-of-1974-system-of-records

National Student Loan Database System (18-11-06). September 9, 2018. 84 FR 47265-47271. https://www.federalregister.gov/documents/2019/09/09/2019-19354/privacy-act-of-1974-system-of-records

Customer Engagement Management System (CEMS) (18-11-11). June 13, 2018. 83 FR 27587-27591. https://www.federalregister.gov/documents/2018/06/13/2018-12700/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 records maintained or transmitted through DCC follow the records disposition schedule for each back-end system. The applicable records schedules are as follows:

ED Records Schedule No. 051 – National Student Loan Data System (DAA-0441-2017-0004) (ED 051). Records are destroyed 30 years after cutoff. Cutoff is annually when an applicable account is paid in full.

ED Record Schedule No. 052 – Ombudsman Case Files (N1-411-09-21) (ED 052). This records schedule is being amended and pending approval by National Archives and Records Administration (NARA). Records will be held indefinitely until the applicable NARA approved amendments are in effect.

ED Record Schedule No. 072 – FSA Application, Origination, and Disbursement Records (DAA-0441-2013-0002) (ED 072). This records schedule is being amended and pending approval by the NARA. Applicable records will be held indefinitely until the applicable NARA approved amendments are in effect.

**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.

PII that is maintained in DCC is used for identification verification and can include basic identifying and contact information such as first and last name, date of birth, phone number, mailing address, email address, and Social Security number (SSN). These PII elements are initially collected through the FAFSA application and can be modified or added to through interactions with DCC. Additionally, information regarding your Federal student loans and other types of aid will be maintained and/or transmitted through DCC.

For a more detailed description of the records that can be collected and transmitted through DCC, please refer to each back-end system's PIA or SORN.

**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 either collected directly from individuals (students/borrowers and/or parents) or is transferred from:
Common Origination and Disbursement (COD)
National Student Loan Database System (NSLDS)
Central Processing System (CPS)
Customer Engagement Management System (CEMS)

**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 directly from the individual either verbally over the phone or electronically via the DCC webpage. Transfers of information between DCC and the back-end systems are done so electronically.

**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?

Data is collected directly from individuals, who are responsible for self-validating the correctness of the information they provide through DCC. Data are revalidated by call-center agents whenever a borrower calls. All other validation of records is the responsibility of the back-end system.

**Use**

**3.6.** Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

PII is used for identification verification and financial aid eligibility determination throughout the student aid lifecycle.

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

No

[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.

**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.

No

**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 initially collected through the FAFSA application and originally maintained in the Central Processing System (CPS). When borrowers access studentaid.ed.gov, the SSN is transmitted to DCC to be used as a unique identifier to access records across the various back-end systems.

**3.8.2.** Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

Other alternatives were considered but SSN remains the most reliable way to match records.

## 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.

Direct notice, prior to collection, is provided during the FAFSA application process at studentaid.ed.gov when PII is collected by the Central Processing System. DCC is a new

system that utilizes this existing notice. Please refer to the CPS PIA for more information.

The DCC website (studentaid.ed.gov) provides additional detailed notice in its privacy policy.

**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://studentaid.ed.gov/sa/privacy - StudentAid.gov

The Privacy Policy for the DCC website is currently being drafted. This section will be updated when the policy is finalized.

**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?

The borrower has the opportunity to initially decline to provide the information; however, providing certain information is required in order to (i) communicate with websites or customer service call centers, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness). If an applicant does not provide all of the information needed to process and service the aid, actions may be delayed or service may be denied.

**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.

No

**5.2.** What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

**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.

No

**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 whom and for what purpose**.

☐ N/A

DCC does not share PII externally, but the PII collected or maintained in DCC may be shared in accordance with an applicable routine use published in the System of Record Notices for the relevant back-end systems.
. Please see question 2.2.1 for more information on applicable SORNs.

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

☑ N/A

Click here to enter text.

**5.7.** Is the sharing with the external entities authorized?

☐ N/A

Yes

[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.

**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

Click here to enter text.

**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

Click here to select.

**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?

A user may access their records by signing into their studentaid.gov account. Additionally, a user may access records by calling the contact center.

Individuals may also contact the System Manager listed in the respective SORN in question 2.2.1 and provide the necessary particulars listed in order to request access to their own information.

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

A user may correct PII displayed on their StudentAid.gov account by logging in and updating the account information. Additionally, a user may access and amend records by calling the contact center.

Individuals can also request corrections or amendments to inaccurate or erroneous PII maintained by the Department by contacting the System Manager listed in the respective SORN in question 2.2.1.

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

Individuals are notified of the procedures for correcting their information through the publication of this PIA, the publication of the back-end systems' PIAs, and through the SORNs referenced in question 2.2.1.

## *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?

The Department of Education and FSA have developed policies and procedures to address technical, administrative and physical safeguards.
Access to the system is controlled via:
Physical security controls such as 24hour security, access controlled areas; electronic access Controls such as different types of accounts, domains, privileged users, and role assignments and account management processes; periodic review of accounts to ensure

there is no unusual activity or prolonged inactivity; ongoing audit log monitoring and review to detect anomalies; identification and authentication processes for both system administrators and borrowers; robust password security rules; Intrusion monitoring and detection and additional firewall rules; Configuration management policies and change review; Security assessments and compliance monitoring; encryption of data in transit and at rest; penetration testing and compliance tests via the security assessment process; and independent validation and verification of security and privacy control descriptions.

**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.

Monitoring, testing, and evaluation are ongoing as FSA follows the Department's Lifecycle Management framework and takes part in the Authority to Operate (ATO) process which includes a rigorous assessment of the security and privacy controls and potential plans of actions and milestones to remediate any identified deficiencies. Additionally, the DCC application, along with the supporting GSS, are scanned regularly using automated tools. The results of the vulnerability scans are reviewed and addressed at the application and infrastructure levels. Annual security assessments are conducted as self-assessments and independent assessments. Intrusion detection and monitoring systems are employed to review accesses and modifications and detect anomalies. Changes are captured and reviewed in audit logs for all software components.

## 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 included the privacy program throughout the development of this new system. Since this is a front-facing system to multiple back-end systems, the system owner in ensures consistency and relevancy with the other relevant PIAs and SORNs. At the moment, all the connected PIAs are being updated to ensure the privacy is

sufficiently protected and the uses of PII are documented. As this system continues to expand to its fully intended capabilities and takes on the functions currently provided by the backend systems, the system owner will work closely with the Privacy team to ensure all required privacy controls, currently in place at the back-end system are implemented at the DCC application level.

**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?

The main privacy risks are the unauthorized access, use, or loss or control of the data which can result in identity theft or other forms of fraud. These risks are mitigated through various safeguards such as access controls, configuration management and anomaly detection, strict password rule and two-factor authentication capabilities and continuous monitoring of intrusion detection and firewall alerts.