Privacy Impact Assessment (PIA)

for the

Digital Customer Care (DCC)

September 23, 2022

For PIA Certification Updates Only: This PIA was reviewed on Enter date by Name of reviewer certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Kimberly Ferguson/Information System Security Officer
Contact Email: Kimberly.Ferguson@ed.gov

System Owner

Name/Title: Pardu Ponnapalli/Information System Owner
Principal Office: Federal Student Aid (FSA), Next Generation Program Office (NGPO)

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 Customer Care (DCC) is an application hosted on the U.S. Department of Education (Department) Federal Student Aid (FSA) Cloud that consolidates several websites, apps, and platforms related to customer care in the student aid process into one system. The DCC platform is accessible at StudentAid.gov and provides a unified platform to assist aid applicants and recipients with all financial aid needs from origination and disbursement to repayment. The DCC includes three components—the Digital Platform, Marketing and Communication Platform, and Customer Care Platform—all accessible at StudentAid.gov.

1. The Digital Platform resides on StudentAid.gov (a public-facing website) and the myStudentAid mobile app. The Digital Platform consolidated content and functionality that was previously available on separate websites such as fsaid.ed.gov, studentloans.gov, nslds.ed.gov, feedback.ed.gov, borrowerdischarge.ed.gov, and fafsa.gov. The Digital Platform provides customers with information on Federal student aid and supports functionality such as creating and maintaining an FSA ID (username and password); completing a master promissory note; completing entrance and exit counseling; applying for loans or repayment plans; viewing grant and loan history; and more.

   PII is either collected directly from individuals (aid applicants, recipients, parents, and/or spouses) or is transferred to and/or from the Department's Access and Identity Management System (AIMS), Common Origination and Disbursement (COD), the National Student Loan Database System (NSLDS), Nelnet/Great Lakes, College Scorecard, Person Authentication System (PAS), Federal Student Aid Information Center (FSAIC), Central Processing System (CPS), Education Data Management Analytics Platforms & Services (EDMAPS), and Business Process Operations (BPOs). In addition to the PII from the systems listed above, the FSA ID that is used to access the Digital Platform also includes PII that is stored in PAS.

Additionally, the Virtual Assistant is a chat bot that employs cognitive artificial intelligence (AI) services across multiple customer channels. These AI services use natural language understanding to answer frequently asked questions and provide key transactional functions (e.g., Loan Balance, Payment Status). The Virtual Assistant interfaces with the Digital Platform and the 1-8004FEDAID Integrated Voice Response (IVR).

2. The Marketing and Communication Platform uses Adobe Campaign to send emails, text messages, and mobile push notifications to customers. Examples of communications include confirmation emails triggered by the completion of a task on StudentAid.gov and reminders to complete the Free Application for Federal Student Aid (FAFSA). The platform also includes Shado, an internally developed application that logs user actions and makes them available to the Customer Relationship Management (CRM) tool to better support callers. Shado stores user interaction data, which consist of web and application log data with user correlation IDs to help identify user website actions.

3. The Customer Care Platform includes the IVR and telephony for 1-8004FEDAid, as well as a CRM tool used by customer service representatives for storing customer interaction data, and other tools used for managing contact centers.

The CRM stores customer interactions with the contact centers for all callers (inbound/outbound phone calls, emails, chats, webform submissions). Data storage for the CRM application includes data about aid applicants, recipients, parents, spouses, and schools. CRM also provides web chat services for the Digital Platform, as well as case management tools that assign, queue, escalate, and resolve customer inquiries.

The CRM standardizes contact management by leveraging integration with Person Master Data Management (PMDM) which is stored in COD. PMDM is the system of record for aid applicants, recipients, parents, and/or spouses, including personal identifiers, demographic attributes, and addresses, phone, and email contact details across the FSA enterprise. PMDM stores a consolidated view of a customer's information, along with historical changes, for COD and DCC.

The customer care platform is used by Business Process Operations (BPOs), which are the contact centers for inquiries from aid applicants, recipients, parents, and/or spouses. The customer service representatives (CSRs) use the customer care platform to access information about customers and provide them service. CSRs authenticate into the CRM using their AIMS credentials. They also have accounts to authenticate onto other contact center tools.

DCC also hosts the Federal Student Aid Estimator, a tool that provides an estimate of what federal student aid an individual may be eligible to receive. While information needs to be provided to the tool to provide a real-time estimate, the tool does not store and/or maintain any user entered data when they complete the estimator workflow.

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

FSA collects PII on individuals throughout the student aid lifecycle for identity verification and financial aid eligibility determination. DCC (accessed through StudentAid.gov) is the front-end customer interface that interacts with the various back-end systems that maintain and process the PII. PII collected via the DCC website will be transmitted, as appropriate, to NSLDS, COD, FSAIC, CPS, EDMAPS, and BPOs. For more information on how records are handled within these systems, please refer to the PIAs and SORNs for each of the listed systems at www.ed.gov/privacy.

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?

Updated PIA

This PIA is being updated as part of the regular review process and to identify changes to the system since the last revision of the PIA.

The following is a major change for DCC: DCC now interfaces with the FSAIC and with the five BPOs. The customer care platform will be used by BPOs, which are contact center operations for customer inquiries, throughout the full student aid lifecycle. BPOs consist of the following vendors:

i. Business Process Operations Ed Financial (BPO-Edfin)
ii. Business Process Operations Frank H. Cann & Associates (BPO-FHC)
iii. Business Process Operations Max (BPO-Max)
iv. Business Process Operations Missouri (BPO-MO)

[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

1.5. 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 information contained in DCC is found within Sections 483 and 484 of the Higher Education Act (HEA) of 1965, as amended.

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

Common Origination and Disbursement System (18-11-02). September 13, 2022. 87 FR 56015. https://www.federalregister.gov/documents/2022/09/13/2022-19888/privacy-act-of-1974-system-of-records

[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

National Student Loan Database System (18-11-06). September 22, 2022. 87 FR 57873. https://www.federalregister.gov/documents/2022/09/22/2022-20682/privacy-act-of-1974-system-of-records

Common Services for Borrowers (CSB) (18-11-16). September 13, 2022. 87 FR 56003. https://www.federalregister.gov/documents/2022/09/13/2022-19887/privacy-act-of-1974-system-of-records

Enterprise Data Management and Analytics Platform Services (EDMAPS) (18-11-22). September 13, 2022. 87 FR 56038. https://www.federalregister.gov/documents/2022/09/13/2022-19886/privacy-act-of-1974-system-of-records

Aid Awareness and Application Processing (AAAP) (18-11-21). September 13, 2022. 87 FR 56026. https://www.federalregister.gov/documents/2022/09/13/2022-19890/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

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 – Ombudsmen Case Files (N1-411-09-21) (ED 052). This records schedule is being amended and pending approval by 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.

General Information

- Full name
- Username
- Social Security number (SSN)
- Taxpayer Identification Number (TIN)
- Student loan account number
- Driver's license number and issuing state
- Citizenship status
- Date of birth
- Contact information
- Home address
- Home, work, alternate, and mobile telephone numbers
- Email address

Household Information

- Family size, dependency status, marital status, spousal identifiers, estimated family contribution

Financial Information

- IRS Data for Income Based Repayments, (adjusted gross income, tax filing status and year, and exemptions), yearly income, credit report information

Employment Information

- Name, Employer Identification Number, address, phone number, website, begin and end date of employment

Loan/Grant Information

- Dollar amount, payment milestones from origination through final payment
- Promissory note information and eligibility information

In addition to the PII elements above, any information provided by customers when contacting DCC will be maintained in this system.

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

Yes

FSA collects the minimum amount of PII required on individuals throughout the student aid lifecycle for identity verification and financial aid eligibility determination. Information accessed through DCC is needed to validate identity and address any questions or issues posed by aid applicants, recipients, parents, and/or spouses. DCC (accessed through StudentAid.gov) is the front-end customer interface that interacts with the various back-end systems that maintain and process the PII.

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 (aid applicants and recipients, parent(s) of a dependent applicant, and/or spouse of a married applicant) or is transferred to and/or from backend Department systems, including:

- AIMS
- COD
- NSLDS
- Nelnet/Great Lakes
- College Scorecard
- PAS

- FSAIC
- CPS
- EDMAPS
- BPOs

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 (StudentAid.gov). Transfers of information between DCC and the backend systems are done electronically. These systems are listed in question 3.3.

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?

Individuals submitting data directly to DCC are responsible for ensuring information provided to the Department is correct. For more information on how data are validated for the systems listed in question 3.3, please refer to their respective PIAs and SORNs.

Use

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

PII is used for identity verification and financial aid eligibility determination. When an aid applicant or recipient creates an FSA ID account using the DCC's StudentAid.gov website or myStudentAid mobile App, the PII entered by the aid applicant or recipient is stored in PAS. This information is used to ensure the correct actions are associated to correct person to validate the caller if they call into a contact center. In addition, information collected also assists in resolving inquiries and questions from aid applicants or recipients.

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

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.

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

SSNs are initially collected through FAFSA and maintained in the CPS. SSNs are accessed by DCC customer representatives as a unique identifier to distinguish the aid applicant or recipient's identity for the customer representative to access records across the various back-end systems. SSNs are used to verify an aid applicant or recipient's identity but not stored within DCC.

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

☐ N/A

Other alternatives (such as customer ID[4]) were considered but the SSN remains the only reliable way to match records. SSNs are accessed by DCC customer representatives as a unique identifier to distinguish the aid applicant or recipient's identity for the customer representative to access records across the various backend systems.

[4] Customer ID is a number assigned to individuals when they submit the FAFSA.

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 CPS. DCC utilizes this existing notice for information brought into DCC from CPS. Please refer to the CPS PIA for more information.

StudentAid.gov, DCC's public-facing website, also includes a privacy policy as linked in Question 4.2.

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

Privacy | Federal Student Aid

The Privacy Policy is listed in the StudentAid.gov website identified above.

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 individual has the opportunity to decline providing 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

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

☑ N/A

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.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

No

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

[5] 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.

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

☑ N/A

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

5.11. Does the project place limitation on re-disclosure?

☑ N/A

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 certain portions of their records (such as FAFSA status) through the IVR portion when calling the call/contact center.

In addition, if an individual wishes to access the content of a record in this system of records, he or she should contact the system manager using full name, address, and telephone number to distinguish between individuals with the same name. The individual must meet the requirements in 34 CFR 5b.5, including proof of identity.

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.

In addition, if an individual wishes to contest the content of a record in this system of records, he or she should contact the system manager using full name, address, and telephone number to distinguish between individuals with the same name, identify the specific items to be changed; and provide a written justification for the change. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

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 backend 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?

Access to the system is limited to authorized DCC program personnel and contractors responsible for administering the DCC program. Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing the DCC program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), DCC must receive a signed ATO from a designated FSA official. FISMA controls implemented by DCC are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

Physical safeguards include the staffing of security guards 24 hours a day, seven days a week, to perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest, access to records is strictly limited to those staff members trained in accordance with the Privacy Act and Automatic Data Processing (ADP) security procedures.

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.

DCC is required to obtain and maintain an ATO. This process includes a tri-annual independent assessment of all required security and privacy controls and produces Plans of Actions and Milestones (POA&Ms) to ensure any deficiencies are remediated. DCC also participates in the Ongoing Security Authorization (OSA) Program and continuous monitoring program. The OSA, which reviews FISMA controls, is conducted quarterly, and the system is scanned continuously to ensure that security and privacy controls are in place and working properly. DCC has a regular patching cycle to ensure the system is secured with the most up to date capabilities.

Following each patch release an additional scan is conducted to ensure continuing operations. Additional activities include conducting regular self-assessments, contingency plan testing and participating in tabletop exercises.

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's risk management framework process to receive an ATO. During the ATO process, DCC makes sure that the National Institute

of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. 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 (LMM), which addresses security and privacy risks throughout the system's life cycle.

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 DCC 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 the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.