Privacy Impact Assessment (PIA)

for the

Business Process Operations (BPO)

July 16, 2021

For PIA Certification Updates Only: This PIA was reviewed on **May 27, 2021** by **Jeremy Dick** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jeremy Dick, Information System Security Officer (ISSO)
Contact Email: Jeremy.Dick@ed.gov

System Owner

Name/Title: Bruce Cruz, Information System Owner (ISO)
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.

This privacy impact assessment (PIA) covers all Business Process Operations (BPO) systems on behalf of Federal Student Aid (FSA). BPOs are the contact center operations for customer inquiries via phone, email, or chat throughout the full student aid lifecycle. The five BPOs utilized by FSA are covered under the same PIA as each BPO is functionally identical, performing the same tasks and maintaining the same types of information. A BPO is a contact center with a facility, customer service representatives (CSRs or agents) in the facility, and desktop computers for the agents. The CSRs connect into the Digital Customer Care (DCC), National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), Debt Management Collection System 2 (DMCS 2) and Person Authentication Service (PAS) systems to respond to borrower inquiries on aid processing. BPOs access borrower PII by accessing these U.S. Department of Education (Department) systems through two methods. BPOs use a desktop suite of tools to access DCC via enablement software. BPOs use web-enabled services to access COD and NSLDS. Authentication for accessing COD and NSLDS is done through Access & Identity Management System (AIMS), while DMCS 2 has its own authentication process.

When a borrower or applicant initiates a call or chat with FSA, the session/call is routed to a BPO agent and the borrower's or applicant's data are pulled up from the DCC system to the agent to assist the caller. Once the call/chat is complete, the records are updated in DCC or in a system connected to DCC through the customer relationship management (CRM) toolset (which is also part of DCC). None of the information is maintained by the agents in the BPO; rather, the information is saved back into DCC after the call ends. The process is very similar for BPOs' use of systems other than DCC; a BPO agent pulls data from a system and updates data in that system once a call or chat is complete. The only difference between the use of DCC and other systems is that DCC is used through desktop applications while the other systems are used through a web browser.

The five BPO vendors are Business Process Operations Edfin (BPO-Edfin), Business Process Operations FHC (BPO-FHC), Business Process Operations Max (BPO-Max), Business Process Operations Missouri (BPO-MO), and Business Process Operations Trellis (BPO-Trell).

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

[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

used, maintained, or shared.

When a borrower or applicant contacts the Department seeking assistance using any of the available contact means (phone, email or chat), the BPO agents will ask the customer for certain PII to verify the customer's identity and to establish a means to resume communications with the individual(s) if the communication is disconnected, in order to resolve their customer's student aid issue, feedback, or complaint.

In addition, the BPOs will obtain the customer's PII via the DCC platform, NSLDS, and COD, in order to assist the customer with their inquiry. The information obtained from these systems will be temporarily available to the BPO; however, the PII will not be permanently maintained in the BPO but will remain resident in the respective systems from which it originates. For more information on how PII is handled in the DCC, NSLDS, and COD, please refer to those individual PIAs and SORNs, which can be found 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?

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 HEA give 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

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

Common Services for Borrowers (CSB) (18-11-16). September 2, 2016. 81 FR 60683
https://www.federalregister.gov/documents/2016/09/02/2016-21218/privacy-act-of-1974-system-of-records

Person Authentication Service (PAS) (18-11-12). March 20, 2015. 80 FR 14981

[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

https://www.federalregister.gov/documents/2015/03/20/2015-06503/privacy-act-of1974-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.

Records maintained or transmitted follow the records disposition schedule for each back-end system. Please see the DCC, NSLDS, COD, and/or DMCS PIAs for additional information.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes
BPOs will not maintain or store PII beyond the time it takes for the BPO to resolve a customer's inquiry during a call, email, or chat session. PII is contained in the underlying systems and follows those records disposal schedule and processes.

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.

Note: BPO does not maintain or store any of the following PII beyond the time it takes for the BPO to resolve a customer's inquiry during a call, email, or chat session.

General Information

- Full name
- User name
- Social Security number
- Taxpayer Identification Number
- 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
- 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

Contractors working as agents in BPOs utilize usernames and passwords to access the system. Other Federal employee/contractor information, such as administrative credentials and identity authentication data, is included in the systems accessed by BPO.

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

Yes

The PII viewed by the BPO agents is used to verify a customer's identity and to resolve the customer's issues. The PII in the systems BPOs access is the minimum necessary to establish and administer student loans. The PII that agents access is the minimum necessary to authenticate the customer and to assist the customer.

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 sourced from:
Common Origination and Disbursement (COD)
National Student Loan Database System (NSLDS)
Digital Customer Care (DCC)
Debt Management Collection System (DMCS)
Personal Authentication Service (PAS)

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 by the BPOs either verbally over the phone or electronically (e.g. chat or email (web form)) via the DCC platform. Transfers of information between DCC and the back-end systems are done electronically. Other systems' data (COD, NSLDS, DMCS) are viewable via web browsers.

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 by the BPOs directly from individuals, who are responsible for self-validating the correctness of the information they provide through DCC, NSLDS, COD, DMCS. Identity of the individual is revalidated from the individual by call center agents whenever a borrower calls, initiates a chat session or web form submission. Integrity of the data 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.

[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.

PII is used for identification verification and to help address the inquiry from a customer who contacts the Department for assistance.

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

No

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.

Yes

While the BPOs do not collect SSNs from customers, the BPO CSR Agents verify the identity of the customer, and therefore have access to the SSNs that are maintained in the systems that agents access to assist customers. If the customer is asking customer-specific information and not general information, the SSN is requested for verification.

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 Free Application Federal Student Aid (FAFSA ®) application and maintained in the Department's Central Processing System. 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. The customer's DOB and SSN are required to match to other financial and disbursement databases to establish the financial and historical accuracy of the customer's claims. These data elements are not stored or maintained in the BPOs

system beyond the time it takes for the BPO to resolve a customer's inquiry during a call, email, or chat session.

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

☑ N/A

While the BPOs do not collect SSNs from customers, the BPOs may have access to SSNs that are maintained in the systems that agents access to assist customers For these back-end systems, there are no feasible alternatives to consider for the collection of SSNs. A valid SSN is required as the unique identifier for students, parents, and financial aid professionals. Additionally, use of the SSN is required as the unique identifier by other external partners involved in determining eligibility for Federal student aid, such as the Internal Revenue Service and other Federal agencies with whom the Department conducts a computer match.

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 for the underlying systems. During a call, email, or chat, the BPO CSR may ask the caller for identifying information to validate the caller's identity when their issue requires looking up a caller's account. Not all issues require identity validation. 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.gov/notices - StudentAid.gov

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 customer has the opportunity to 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. https://studentaid.gov/notices/privacy

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

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

[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.

5.6. 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

Click here to enter text.

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

☑ N/A

Click here to enter text.

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

Click here to select.

6. Redress

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

A user may access their records by logging into their studentaid.gov account or by calling the contact center. For information contained in a Privacy Act system of records listed in Section 2.2.1, users may make a Privacy Act request for access. The request must meet the requirements of 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. For information contained in a Privacy Act system of records listed in Section 2.2.1, users may request inaccurate information be corrected by making a Privacy Act request. The request must meet the requirements of 34 CFR 5b.5, including proof of identity.

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 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 24-hour security, access-controlled areas, identification and authentication processes for both system administrators and borrowers, electronic access controls such as different types of accounts, domains, privileged users, and role assignments and account management processes. FSA conducts periodic review of accounts to ensure there is no unusual activity or prolonged inactivity, as well as ongoing audit log monitoring and review to detect anomalies. Additional controls include robust password security rules, intrusion monitoring and detection, 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 implementation.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every FSA system must receive a signed Authorization to Operate (ATO) from a designated authorizing official. The ATO process includes a rigorous assessment of security controls, plans of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program.

FISMA 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, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

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.

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 self-assessments.

Additionally, the BPOs (BPO-Edfin, BPO-FHC, BPO-Max, BPO-MO and BPO-Trell) and the DCC application (under a separate ATO), are scanned at least monthly using automated tools. The results of the vulnerability scans are reviewed and addressed. Self-assessments and independent assessments are conducted annually. 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 FSA privacy office and the Departent's privacy office throughout the development of this new system. Since this is a front-facing system to multiple back-end systems, the system owner ensures consistency with the other relevant PIAs and SORNs.

The system owner ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the statute and the provisions of the Federal Records Act. In addition, the system owner ensures continued compliance with all Departmental policies and the relevant SORNs, and ensures appropriate security and privacy controls are implemented to restrict access and 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 information system security officer, and participates in FSA's Lifecycle Management Methodology, which addresses security and privacy risks throughout the system's life cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as SORNs, memorandum of understanding, and interconnection security agreement.

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 primary risk posed by this system is the unauthorized disclosure or use of PII. 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 cost.

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. Such safeguards include those administrative, technical, and physical safeguards addressed in Section 7.3. Additional controls include access controls, configuration management and anomaly detection, strict password rules, two-factor authentication capabilities, continuous monitoring of intrusion detection and firewall alerts, updating the security patches and software throughout a continuous monitoring process, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department.