Privacy Impact Assessment (PIA)

for the

Common Origination and Disbursement

March 17, 2020

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: Laura Malinski/Information System Security Officer
Contact Email: laura.malinski@ed.gov

System Owner

Name/Title: Diana O'Hara/System Owner
Principal Office: Federal Student Aid

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.

The Common Origination and Disbursement (COD) system processes Federal financial aid programs for Title IV schools for the U.S. Department of Education, Office of Federal Student Aid (FSA). The COD processing system initiates, tracks and disburses funds to eligible students and schools and contains records of individuals who apply for a Federal grant or loan under one of the programs authorized under title IV of the HEA, including:

- Pell Grant
- Iraq and Afghanistan Service Grant (IASG)
- Direct Loan (Federal Direct Stafford/Ford Loans; Federal Direct Unsubsidized Stafford/Ford Loans; Federal Direct PLUS Loans; Federal Direct Consolidation Loans)
- Teacher Education Assistance for College and Higher Education Grant (TEACH)
- Federal Perkins Loans Program
- National SMART Grant Program
- Federal Family Education Loan (FFEL) Program
- Federal Insured Student Loan (FISL) Program
- Auxiliary Loans to Assist Students (ALAS) Program
- Health Professions Student Loan (HPSL) Program
- Health Education Assistance Loan (HEAL) Program

In addition, the COD system provides the financial management, program management and communication functions for the Campus Based programs, including Federal Perkins Loan, Federal Work-Study and the Federal Supplemental Educational Opportunity Grant. The COD application standardizes school participation in various financial aid programs by combining the screens for the individual financial aid programs and creating one single process for schools to obtain financial aid for their students. COD also supports FSA' s objective of achieving an enterprise-wide solution that provides real-time data to students, schools, and financial partners via web portals.

Using the applicant-level information along with data regarding school and program eligibility, schools access the system and build student awards (Grants and Loans) based

on criteria established by the United States Congress and Federal Student Aid. Once the awards are submitted, COD processes these transactions, posts down-stream effects to the appropriate interface partners and creates reports for FSA and schools.

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

The PII contained in this system is used for the following purposes:

- To determine recipient eligibility and benefits for Federal grant or loan programs;
- To store electronic data that support the existence of a legal obligation to repay funds disbursed under Federal grant or loan programs;
- To identify whether an individual may have received a Federal grant or loan at more than one educational institution for the same enrollment period or exceeded the annual award limits in violation of program regulations;
- To identify an individual who completed a Special Direct Consolidation opportunity application and promissory note; counseling for Direct Loan and TEACH Grant programs; an electronic request to repay a Direct Loan under an income-based or income contingent (hereafter "income-driven") repayment plan; or the electronic Federal Direct Consolidation Loan Application and Promissory Note;
- To track the level of study, Classification of Instructional Program (CIP) code (field of study), and educational program length to limit eligibility for Direct Subsidized Loans, to enable Federal Loan Servicers to determine the periods for which a borrower will be responsible for the accruing interest on outstanding Direct Subsidized Loans, and to track student enrollments by educational program for purposes of determining educational program outcomes, including using that information to obtain average earnings of students by educational program from another Federal agency.
- To enable an institution of higher education to reconcile, on an aggregate and recipient-level basis, the amount of Federal grant and Direct Loan funds that an institution received with disbursements it made to, or on behalf of, eligible students; and to request on-line credit checks to determine the credit worthiness of a borrower for Federal Loans;
- To assist an institution of higher education, a software vendor, or a third-party servicer with questions about a Federal grant or loan;
- To assist an institution of higher education with student loan default prevention;

[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

- To reconcile school cash drawdowns from the U.S. Department of the Treasury to institutions of higher education reported disbursements and to ensure the respective institutions of higher education receive the appropriate amount of dollars during the respective time period.

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

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 Higher Education Act of 1965 (HEA), as Amended, section 441 and 461 Title IV, section 401;
- Executive Order 13478—Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers;
- 31 U.S.C 7701, Taxpayer Identifying Number

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 (COD) System (18-11-02) was last published in the Federal Register on August 16, 2019 at 84 FR 41979-41987. https://www.federalregister.gov/documents/2019/08/16/2019-17615/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 Common Origination and Disbursement will follow the "FSA Application, Origination, and Disbursement Records" records schedule.
Schedule Locator No: 072
Approved Date: 04/14/2014
Title: FSA Application, Origination, and Disbursement Records
NARA DISPOSITION AUTHORITY: DAA-0441-2013-0002

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

[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

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.

The COD system receives:

- Full name
- Social Security Number
- Student Loan account number
- Driver license number and issuing state
- Citizenship status
- Date of Birth
- Contact Information
    - Home address (current address); home, work, alternate, 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, Website, Begin & End Date of employment
- Loan/Grant Information
    - Dollar amount, payment milestones from origination through final payment, Promissory Note information
- Eligibility Information
    - Level of study, CIP code (field of study), length of educational program

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.)?

COD primarily receives PII from the following FSA systems. For more information on these systems, please refer to their individual PIAs and SORNs:

- The Central Processing System (CPS)/studentaid.ed.gov
- The National Student Loan Data System (NSLDS)
- The Postsecondary Education Participants System (PEPS)
- The Common Services for Borrowers System (CSB)/Title IV Additional Servicers and Not for Profit Collection Agencies
- Student Aid Internet Gateway (SAIG)
- Debt Management Collection System (DMCS)
- Digital Customer Care (DCC)

These systems directly obtain records from the individual or from institutions of higher education. For Direct Loan PLUS loans, COD also receives credit check information from credit bureaus.

Additionally, COD may obtain PII directly from individuals.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The information is collected via:

- Electronic transmission of bulk file transfers from the FSA systems listed above
- Studentaid.ed.gov for borrower facing interactions
- Phone calls, chat, and other forms of correspondence with customer service agents through the Digital Customer Care platform
- Electronic transmission from credit bureaus

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?

The information is validated initially at the source systems that provide PII to COD. PII is additionally validated via recipient-initiated communication with customer service

[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.

agents, verification between internal databases within systems, and data exchange with external trading partner databases such as:

- Credit Bureaus
- Loan Servicers
- Directory Assistance
- Educational Institutions

Use

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

COD uses this student-level detail to book loans, account for awarded grants and to enable the Department to reconcile school cash drawdowns from the Treasury to individual student disbursements. This information is used to ensure the respective schools receive the appropriate amount of financial aid dollars for their students during the respective time periods.

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

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 the unique identifier for title IV, HEA programs and is required by program participants and their trading partners to satisfy borrower identification, borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. The SSN is the required identifier for numerous business processes.

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

☐ N/A

To the extent possible, COD employs the use of other unique identifiers in lieu of the SSN, such as account numbers, but the SSN is the required identifier for numerous business processes. Trading partners including the Internal Revenue Service for use of the Data Retrieval Tool, institutions of higher education, credit bureaus, lenders and servicers utilize the SSN as a primary identifier.

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.

COD provides notice to individuals directly accessing its website.:

COD also provides a Privacy Act Notice with all their disclosure statement correspondence, borrower acceptance letters and endorser packages. In addition, there is a link to the privacy policy on the Student Loans webpage, which is the student facing portion of the system of record providing additional notice on the handling of PII.

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://cod.ed.gov/cod/Privacy
https://studentaid.gov/notices/privacy

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?

Providing information is voluntary however COD is a part of the Student Aid Lifecycle and individuals do not have the ability to specifically decline to provide information or opt out of their information being maintained in COD. Opportunities to decline to provide PII or opt out are at the initial point of collection.

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.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

COD will share PII associated with the Master Promissory Notes with the Department's Office of Inspector General (OIG).

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

☑ N/A

Information is shared with OIG to conduct audits.

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.

Yes

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

COD shares borrower name and SSN with loan servicers and name, SSN, date of birth, address and phone number with credit bureaus. Additionally, through the use of the Data Retrieval Tool, COD will share name, SSN, and date of birth with the IRS.

PII may also be disclosed to institutions of higher education; financial institutions; guaranty agencies; software vendors; third party servicers; and Federal, State, tribal or local agencies. More information can be found in the SORN referenced in 2.2.1.

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

☐ N/A

PII is shared with loan servicers in order to ensure borrowers loans are serviced.

PII is shared with credit bureaus in order to perform credit checks on a parent or borrowers during the processing of Direct Loan PLUS Loans.

PII is shared with the IRS in order to authenticate a borrower to access their most recent tax information.

Finally, PII may be disclosed pursuant to one of the following programmatic disclosures as published in the SORN referenced in 2.2.1:

- To verify the identity of the recipient involved or the accuracy of the record, or to assist with the determination of program eligibility and benefits such as identify whether an individual may have received a title IV, HEA Federal grant or loan at more than one institution of higher education for the same enrollment period or may have exceeded the annual award limits under the title IV, HEA Federal grant or Direct Loan programs in violation of title IV, HEA regulations;
- To store electronic data that supports the existence of a legal obligation to repay funds disbursed under title IV, HEA programs, including documentation such as promissory notes and other agreements;
- To enable institutions of higher education to reconcile, on an aggregate and recipient-level basis, the amount of title IV, HEA Federal grant and Direct Loan

[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.

funds that an institution received with the disbursements it made to, or on behalf of, eligible students and request online credit checks to determine the eligibility of applicants or borrowers for a title IV, HEA Federal Direct PLUS Loan;

- To assist individuals, institutions of higher education, third-party servicers, or software vendors with questions about a title IV, HEA Federal grant or loan,
- To support the investigation of possible fraud and abuse and to detect and prevent fraud and abuse in title IV, HEA Federal grant and loan programs,
- To assist institutions of higher education with student loan default prevention,
- To assist the Department in complying with requirements that limit eligibility for Direct Subsidized Loans, and for determining eligibility for a PLUS loan.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

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

Information shared outside of the Department of Education is shared through secure encrypted transmission. External users (e.g., contractors, school financial aid officers) access our systems and data using a username and password from Access & Identity Management System (AIMS), and/or a Department of Education issued Personal Identity Verification (PIV) card. External partners use a secure data transmission of machine-to-machine transfer with external partners such as skip-tracing vendors.

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

Yes

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?

Students/parents can log into www.studentaid.gov to access their information that is shared with COD by CPS.

Also, individuals may contact the system manager providing necessary particulars of your name, DOB, SSN, and any other identifying information requested by the Department to access their records.

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

Students/parents can log into www.studentaid.ed.gov to correct inaccurate or erroneous information.

Individuals may also contact the system manager and provide your name, DOB, and SSN. Identify the specific items to be changed and provide a written justification for the change.

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

The SORN listed in Question 2.2, explain the procedures for correcting an individual's information.

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?

Physical access to the sites of the Department's contractors, where this system is maintained, is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge. All contract and Department personnel who have facility access and system access must undergo a security clearance investigation. Individuals requiring access to Privacy Act data are required to hold, at a minimum, a moderate-risk security clearance level. These individuals are required to undergo periodic screening at five-year intervals. In addition to undergoing security clearances, contract and Department employees are required to complete security awareness training on an annual basis.

Training is required to ensure that contract and Department users are appropriately trained in safeguarding Privacy Act data. The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a "need-to-know" basis and controls individual users' ability to access and alter records within the system. All users of this system of records are given unique user identification. The Department requires the enforcement of a complex password policy and two factor authentication. In addition to the enforcement of the complex password policy, users are required to change their password at least every 90 days in accordance with the Department's information technology standards.

Physical security of electronic data will be maintained in a secured data center, access to which is controlled by multiple access controls.

Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of transmitted data and storage volumes are encrypted.

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.

Monthly authenticated network and operating vulnerability scans are conducted to ensure the security of the COD network environment. Security audits are performed on an annual basis by authorized third parties to ensure the in-place controls are effectively securing the data. The COD application participates in the Ongoing Security Authorization (OSA) program. The objectives of OSA are to provide oversight and monitoring of the security controls in FSA information systems on an ongoing basis, inform the authorizing official (AO) when changes occur that might affect the security of a system, and inform risk-management decisions. FSA evaluates information about new threats and vulnerabilities as it becomes available, and adjusts security requirements or individual controls as needed to maintain authority to operate. This approach allows FSA to understand and respond to the fluctuations of its dynamic security risk posture and reduce inefficiencies in the traditional SA approach. OSA consists of security control assessments and remediation actions.

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 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 provisions of the Federal Records Act, Departmental policies, the Privacy Act and the published SORN, 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 systems' life cycle. Additionally, the system owner

regularly reviews signed agreements that govern data use between organizations, such as System of Records notices, memorandum of understanding, etc.

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 COD 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 theft, embarrassment or financial loss. Organizational harm may include a loss of public trust, legal liability or remediation costs. The risks are mitigated by granting access to only authorized individuals based on their respective position and need to know basis, limited to users who are screened and approved, utilizing least privilege principles, masking SSNs when viewed, encrypting data in transmission and at rest, and updating security patches per the patch schedule and updating devices' operating software and other software.