Exhibit L

Privacy Impact Assessment (PIA)
for the

Common Origination and Disbursement
September 29, 2023

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: Balaji Mysore / Information System Security Officer
Contact Email: Balaji.Mysore@ed.gov

System Owner

Name/Title: Folajimi Ayodele / Information System Owner
Principal Office: Federal Student Aid

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

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 information for various purposes relating to determining eligibility for Federal student financial assistance under programs authorized by title IV of the Higher Education Act of 1965, as amended (HEA); the participation of institutions of higher education (IHE) administering title IV, HEA programs; and the Department's oversight of title IV, HEA programs. COD originates and disburses funds to eligible aid applicants and recipients for the following financial aid programs:

- Federal Pell Grant Program
- Federal Perkins Loans Program
- Teacher Education Assistance for College and Higher Education (TEACH) Grant Program
- Iraq and Afghanistan Service Grant (IASG) Program
- Direct Loan Program, which includes Federal Direct Stafford/Ford Loans, Federal Direct Unsubsidized Stafford/Ford Loans, Federal Direct PLUS Loans, and Federal Direct Consolidation Loan
- Federal Family Education Loan (FFEL) Program
- Federal Insured Student Loan (FISL) Program
- Federal Work Study (FWS) Program
- Federal Supplemental Education Opportunity Grants (FSEOG) Program

These programs are awarded at the IHE level, so the IHE is responsible for providing funds to specific aid recipients, differing from other types of Federal student aid.

The COD system maintains certain records in order to properly execute the aforementioned programs. These records include:

- Student aid applicants' and recipients' information under title IV of the HEA,
- Parent information of dependent aid applicants and recipients,
- Spouse information of aid applicants and recipients, and
- Public Service Loan Forgiveness (PSLF) program records.

Title IV Aid Programs

The COD system provides schools with a process for requesting, processing, disbursing, reporting, and reconciling title IV funds. The COD system receives, processes, and responds to documents submitted by IHEs for Federal Student Aid programs: Direct Loans (DL), Pell Grants, IASG, TEACH Grants, and other programs as required. Direct Loans include Direct Subsidized Loans and Direct Unsubsidized Loans made to eligible students as well as Direct PLUS Loans made to parents of undergraduate students and graduate/professional students. The COD system also maintains and manages school and program funding levels as well as managing school disbursements.

The COD system is responsible for accepting and processing awards within the Federal Student Aid Lifecycle. Federal Aid information is accepted from applications from aid applicants or receipents and school submitted financial aid packages. This requires two business processes that enable the completion of providing aid applicants with financial awards and ultimately completing the processes required to make that aid available:

(1) Loans and Grants Processing – the process of submitting and processing origination and disbursement records for designated federal student aid programs, from participating schools, and for eligible students.

(2) Funds Management – the process of providing the funds to schools to disburse the awards to students and all appropriate program requirements are met.

Campus-based Programs
Some of the financial aid programs mentioned above (e.g., Federal Perkins Loans Program, FWS Program, and FSEOG Program) are considered campus-based programs because they are administered directly by the financial aid office at each IHE. For those programs, the campus-based program lifecycle begins when the program in the COD system is “rolled over” for the upcoming year, and the new Fiscal Operations Report and Application to Participate (FISAP) form becomes available for IHE submission to the Office of Federal Student Aid (FSA) at the U.S. Department of Education (Department). From there, a series of processes and other supplemental forms and deadlines pertinent to each of the college-based programs take place over the course of the lifecycle, spanning roughly August through April.

COD includes the following components:

- COD Web – The COD website (cod.ed.gov) is used by IHEs, financial institutions, and customer service representatives (CSRs) to support the review and modification of data based upon pre-determined roles and permissions. Authentication of users is performed through FSA’s Access and Identity Management System (AIMS).
- COD Batch Application – IHEs, financial institutions, and other FSA systems, as noted below, provide COD batches, which are one or more data records submitted together. The records include student, award, and disbursement information. COD manages the file processing of these data.

- COD-Digital Customer Care (DCC) Servicer Lookup Interface (LDE) -- The interface is a webservice interface in which the DCC platform makes a request to COD for information about an aid recipient's loan servicer. COD responds to DCC with the requested loan servicer data.
- Alerting Services (xMatters) – COD makes use of the xMatters, which is a software-as-a-service (SaaS) solution for receiving and sending alerts to COD support personnel to resolve system issues. Specifically, xMatters receives alerts from the COD system and distributes them to appropriate personnel based on predefined rules. These alerts include job failures, file processing issues and storage usage, and similar system alerts.
- Customer relationship management (CRM) application – This application is used by CSRs to provide customer service for IHEs and partners by responding to questions received by COD and other FSA system users. The tool is a SaaS using the Oracle Service Cloud (OSC). The OSC CRM captures calls, chats, and cases, which include contact information about the aid applicant or receipent.
- COD Contact Centers – COD contact centers includes two sites, ASM Research and Senture. These centers are staffed with resources for handling issues and questions from IHEs via phone and web chat. Contact center staff at each site make use of data from the CRM application and COD Web for contact handling.
- Print input service – This service processes paper correspondence received, including Master Promissory Notes (MPN), endorser documents, as well as paper-based FISAP forms received by COD School Services. Once documents are received, they are scanned and sent to COD in batch format.
- Print output service – This service allows for the printing of paper correspondence related to COD mailed from the Department, such as Program Year closeout letters.

IHEs

IHE users (representatives of IHEs) directly interact with COD using COD Web to perform functions relating to aid origination, disbursement, research and verification, and specific workflows that support program reporting and requirements. IHE users are able to search for individuals affiliated with their institutions to obtain information on loans and grants held by those individuals. IHEs are able to view all information received from a student's Free Application for Federal Student Aid (FAFSA®) through the search function in COD.

IHEs also submit records regarding award information, which COD will either accept or reject based on whether the IHE's records match FSA's records. If rejected, IHEs can use COD Web tools to determine the cause for rejection. For example, if an IHE submits records and finds that they are accounting for $1,000 short of the expected aid the IHE is expected to provide, COD will reject the submission.

IHEs can then use tools within COD to research and verify requests for aid related to their institution to find the missing information and adjust their records accordingly. Aid recipients and applicants do not have access to COD; they may access information stored in COD through DCC.

Financial Institutions (Loan Servicers)

Records submitted by IHEs must also match records maintained by loan servicers. If there is a discrepancy between IHE records and servicer records, loan servicers access COD Web to view information on rejected submissions. Like IHEs, loan servicers can research reasons for rejection. Once a discrepancy is resolved, loan servicers accept the previously rejected submissions. Loan servicers can also view general information regarding awards that they are servicing.

CSRs

CSRs have access to COD Web in order to view information relating to aid origination, disbursement, research and verification, and specific workflows that support program reporting and requirements. CSRs assist IHE users to research any questions related to IHE information, aid applicant and recipient information, and any origination and disbursement rejects.

In addition, CSRs access the CRM to respond to technical issues arising from use of the systems covered by the CRM, which include COD. Users contact the CRM via phone call, web form, or live chat. Name and email address are the only personally identifiable information elements solicited for all contact with the CRM, though other elements may be collected on a case-by-case basis. Contact information (user credentials) is prepopulated in requests when contact with CRM CSRs is made through COD Web.

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

[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

The information maintained in this system is used for the following purposes related to aid applicants and recipients under title IV of the HEA:

1. To determine and validate aid applicants' and recipients' eligibility for and benefits under title IV of the HEA program, HEA programs, including, but not limited to, receiving a loan, grant, or scholarship, and obtaining discharge of eligible loans under title IV of the HEA;
2. To store data and documentation, including, but not limited to, promissory notes and other agreements that evidence the existence of a legal obligation to repay funds disbursed under title IV of the HEA program, HEA programs and alternative documentation of income (ADOI) used to support the calculation of a monthly payment amount income-driven repayment (IDR) plans;
3. To identify whether an aid recipient may have received title IV of the HEA program, HEA program funds at more than one educational institution for the same enrollment period in violation of title IV of the HEA program, HEA program regulations;
4. To identify whether an aid recipient may have exceeded title IV of the HEA program, HEA program fund award limits in violation of title IV of the HEA program, HEA program regulations;
5. To identify an aid applicant or recipient who completed an electronic Direct Consolidation Loan Application and promissory note or a Special Direct Consolidation Loan Application and promissory note;
6. To identify an aid applicant or recipient who completed entrance and exit counseling in the Direct Loan or TEACH Grant programs;
7. To identify an aid recipient who completed an electronic request to repay a Direct Loan, a Department-held Perkins loan, or a Department-held FFEL Program loan under income-driven repayment plans;
8. 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;
9. To maintain a qualifying employer database to allow aid recipients who apply for PSLF, Temporary Expanded Public Service Loan Forgiveness (TEPSLF), or the limited PSLF waiver to search for and select their PSLF qualifying employer;
10. To enable the Department, or other Federal, State, Tribal, or local government agencies, to investigate, respond to, or resolve complaints concerning the practices or processes of the Department and/or the Department's contractors, and to investigate, respond to, or resolve aid applicant and recipient requests for assistance or relief regarding title IV, HEA program funds;
11. To enable an aid applicant, recipient, and, where applicable, an endorser, to

initiate online credit checks when they complete the electronic Federal Direct PLUS Loan Application or an Endorser Addendum;

12. To identify an aid recipient obligated to repay title IV, HEA program funds pursuant to various maintained data and documentation such as promissory notes, applications, and agreements;
13. To identify an aid recipient who received a FSEOG or who earned money under the FWS program for use in the calculation of the Student Aid Index (SAI) and to assist with expenditure reporting on the FISAP;
14. To enable an aid recipient to complete a PSLF application using the "PSLF Help Tool" and to maintain the aid recipient's PSLF qualifying employer's information including, but not limited to, authorizing official's name, title, phone number, email address, and digital signature (including time and date stamp); and
15. To identify whether an aid recipient (and where applicable the spouse) who is applying or recertifies eligibility for an IDR plan has or has not provided consent/affirmative approval both to redisclose Federal Tax Information (FTI) of such individuals pursuant to clauses (iii), (iv), (v), and (vi) of section 6103(l)(13)(D) of the Internal Revenue Code (IRC) of 1986 and under subsection 494 (a) of the HEA (20 U.S.C. 1098h(a)) for the purpose of determining eligibility for, or repayment obligations under, IDR plans under title IV of the HEA with respect to loans under part D of the HEA (the Direct Loan Program), and redisclosure of FTI under IRC § 6103(l)(13)(A) and (C).

The information in this system is also maintained for the following purposes relating to IHEs participating in and administering title IV, HEA programs:

1. To enable an IHE to reconcile, on an aggregate and recipient-level basis, the amount of title IV, HEA program funds that an institution received for disbursements it made to, or on behalf of, eligible students (including reconciling verification codes, reconciling the funds received with disbursements made by type of funds received, and making necessary adjustments);
2. To enable an institution of higher education to request online credit checks on an aid applicant, recipient, or endorser in connection with the determination of the aid applicant's eligibility for a title IV, HEA Federal Direct PLUS Loan;
3. To assist an institution of higher education, a software vendor, or a third-party servicer with questions about title IV, HEA program funds;
4. To assist an institution of higher education with student loan default prevention;
5. To reconcile an institution of higher education's cash drawdowns from the U.S. Department of the Treasury with its reported disbursements and to ensure that the institution of higher education receives the appropriate amount of funds during the respective time period;

6. To collect Campus-Based expenditure information for the previous award year and the ability to apply for Campus-Based program funds using the FISAP; and
7. To enable an institution of higher education to report an aid recipient's receipt of a FSEOG or earnings under the FWS program, which will be used in the SAI calculation and to assist with expenditure reporting on the FISAP.

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

The PIA is being updated as part of the biennial review cycle.

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 under which the system is maintained is title IV of the HEA (20 U.S.C. 1070 et seq.), the Higher Education Relief Opportunities for Students Act of 2003 (20 U.S.C. 1098(b) (including any waivers or modifications that the Secretary of Education deems necessary to make to any statutory or regulatory provision applicable to the student financial assistance programs under title IV of the HEA to achieve specific purposes listed in the section in connection with a war, other military operation, or a national emergency), the FAFSA Simplification Act (title VII, Division FF of P.L. 116-260) (including but not limited to the following sections of the FAFSA Simplification Act: Subsection 702(m), which amends Section 483 of the HEA, and Section 703, which amends Section 401 of the HEA), and the FAFSA Simplification Act Technical Corrections Act (Division R of the Consolidated Appropriations Act, 2022 (P.L. 117-103)).

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

The SORN, titled "Common Origination and Disbursement System (COD)," 18-11-02, 88 FR 41942, was published in the Federal Register on June 28, 2023.

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.

COD falls under the "FSA Application, Origination, and Disbursement Records" records schedule. The schedule locator number is 072, and the approved date is April 14, 2014. The NARA disposition authority ID is DAA-0441-2013-0002. The Disposition Instructions include destroying or deleting Student Application Records 15 years after final repayment or audit of student financial obligation and destroying or deleting Loan Origination and Disbursement Records 15 years after final repayment or audit, or after relevant data is transferred to an alternate recordkeeping system.

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

Yes

[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

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.

Records in COD include, but are not limited to, the following data about aid applicants and recipients, endorsers, aid applicants' and recipients' parents, and spouses of aid applicants and recipients who are part of an aid applicant's title IV of the HEA program, HEA aid application or receive title IV of the HEA program, HEA aid:

- Identifier information, including name, Social Security number (SSN), date of birth (DOB), mailing address, email address, driver's license number, and telephone number;
- Aid applicant and recipient demographic information, including demographic information of the aid applicant's and recipient's parent(s) and aid applicant's and recipient's spouse (if applicable), incarcerated student indicator flag, expected student enrollment, list of participating title IV, HEA institutions of higher education designated by the aid applicant to receive the FAFSA form data along with residency plans, and the financial profile of an aid applicant, an aid applicant's parent(s), or an aid applicant's spouse, as reported and calculated through the FAFSA form, and to also include processing flags, indicators, rejections, and overrides; and the consent/affirmative approval to disclose personally identifiable information to the IRS and to obtain FTI in order to determine eligibility for, or repayment obligations under, IDR plans pursuant to subsection 494 (a) of the HEA (20 U.S.C. 1098h(a));
- Aid recipient's loan information including information about Direct Loans, FFEL program loans, Perkins loans, and FISL program loans. This includes information about the period from the origination of the loan through final payment, and milestones, including, but not limited to: discharge, consolidation, or other final disposition including details such as loan amount, date of disbursement, disbursement amounts, balances, loan status, repayment plan and related information, collections, claims, deferments, forbearances, refunds, and guaranty agencies, lender(s), holder(s), and servicer(s) of an aid recipient's FFEL program loan(s);
- Information about Federal grant aid recipients, including recipients of Pell Grants, TEACH Grants, Iraq and Afghanistan Service Grants, and FSEOGs, including grant amounts, grant awards, verification status, lifetime eligibility used (LEU), IASG eligible veteran's dependent indicator, Children of Fallen Heroes Scholarship eligibility indicator, Pell Grant additional eligibility indicator, approved Prison Education programs (PEPs) (the FAFSA Simplification Act

allows for expanding access to Federal Pell Grants to include Federal and State penal facilities' approved PEPS; and information about the FWS program, including the amount of FWS earnings and category/type of FWS employment;

- Pell Grant collection status indicator and overpayment collection information
- Promissory notes including promissory note identification numbers, loan type, current servicer, principal balance, and the accrued interest for Direct Loans, Federal Direct PLUS Loans, or Department-held FFEL program loans
- TEACH Agreements to Serve elements include name, SSN, date of birth, mailing addresss, email address, driver’s license and telephone number.
- Direct Loan Entrance Counseling forms, Federal Student Loan Exit Counseling forms, Federal Direct PLUS Loan Counseling forms, the Annual School Loan Acknowledgement (ASLA), Federal Direct PLUS Loan Requests, endorser addendums, and counseling in the Direct Loan and TEACH Grant programs, such as the date that the aid applicant completed counseling. The elements include name, SSN, date of birth, mailing addresss, email address, driver’s license and telephone number.
- Credit report information for Federal Direct PLUS Loan applicants, recipients, and endorsers and if applicable, documents related to a Federal Direct PLUS Loan applicant's request for a credit appeal including credit check details, adverse credit history, credit bureau information, and applicant provided appeal support documentation and the Department's appeal decision
- Aid applicant, endorser, or spouse identifier information for a paper or electronic request to repay or annual recertification of an Direct Loan or Department-held Perkins or FFEL loans or annual recertification of eligibility for, an IDR plan, such as SSN; the date that the IDR plan application was completed; ADOI; IDR monthly payment amount based on the plan selection (as applicable); and current loan balances
- Electronic Direct Consolidation Loan or Special Direct Consolidation Loan aid recipient identifier information, such as the aid recipient's SSN, the date that the aid recipient completed the Federal Direct Consolidation Loan application and promissory note, and current loan balances
- Information concerning the date of any default on a loan
- Demographic and contact information for aid recipient accounts that the Department places with the Federal Loan Servicer(s) for collection of the aid recipient's title IV, HEA loans
- Information obtained pursuant to matching programs or other information exchanges with Federal and State agencies, and other external entities, to assist in identifying aid recipients who may be eligible for benefits related to their title IV, HEA loans or other title IV, HEA obligations, including, but not limited to, Total and Permanent Disability discharges, loan deferments, interest rate reductions,

PSLF, and other Federal and State loan repayment, discharge benefits, or for the purpose of recouping payments or delinquent debts under title IV, HEA programs

- Information provided and generated through customer interactions with contact center support via inbound and outbound channels (phone, chat, webform, email, customer satisfaction survey, fax, physical mail, and digital engagement platforms). Information includes, but is not limited to: chat transcripts, email communications, audio recordings of customer calls, and screen recordings of contact center desktop support during customer interactions; and
- Borrower defense (BD) information including a uniquely generated internal system case ID, a uniquely generated BD case number for Department, educational institution and student tracking, Office of Postsecondary Education Identification Number (OPEID), and the applicable regulatory year and provisions (i.e.,1995, 2016, or 2020) under which the BD case is being processed

The system also contains the following data about students provided by IHEs that participate in an experiment under the Experimental Sites Initiative: award year, experiment number, Office of Postsecondary Education Identification (OPEID), student SSN, student last name, and any data collection instrument elements authorized under the Information Collection Request associated with each experiment.

The system also contains records from 2014–2021 on the level of study, Classification of Instructional Program code (field of study), and published length of an educational program in which a student receiving title IV, HEA Federal student aid was enrolled to limit their eligibility for Direct Subsidized Loans to no more than 150 percent of the published length of the educational program in which the student was enrolled, and to determine when an aid recipient who enrolled after reaching the 150 percent limit would have been responsible for the accruing interest on outstanding Direct Subsidized Loans.

The system also contains an aid recipient's PSLF qualifying employer's information including, but not limited to, authorizing official's name, title, phone number, email address, and digital signature (including time and date stamp).

Finally, the system maintains cohort default rates calculated by the National Student Loan Data System (NSLDS) from guaranty agency-reported and Federal Loan Servicer-reported data at the institution level.

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

Yes

The PII collected and maintained is the minimum amount required by COD in order to originate and disburse funds to eligible aid recipients for the financial aid programs listed above in question 1.1. COD utilizes the PII to uniquely identify individuals that apply for aid under the title IV of the HEA and to track the status of applicants and recipients. Additionally, COD is used by IHEs, loan servicers, and CSRs to view the current status of applicants and recipients which requires the use of PII to uniquely identify them.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

COD interfaces with multiple Department and external systems to transmit or receive information necessary to process federal student aid. COD does not interact with the public directly. Rather, aid recipients and applicants provide their information to FSA through other FSA systems which are then shared with COD where necessary.

Internal Department systems/offices:

- **Access and Identity Management System (AIMS) -** The AIMS interface is an indirect browser-based interface that is used for authentication of COD Web users. AIMS is hosted at the FSA data center and is a web service designed to authenticate web users logging into the COD Web website.
- **Central Processing System (CPS)** - COD automatically generates and sends Grant Recipient File information, which includes individual Pell recipient summary level data, to CPS. The Demographic Data Exchange (DDE) file, which includes individual CPS transaction data, is sent back to COD for reporting purposes.
- **DCC**:
  - COD receives Income-Driven Repayment (IDR) plans, Master Promissory Notes, Plus Promissory Notes, loan consolidation, counseling transactions for Direct Loan, TEACH and Parent PLUS counseling, and PSLF information from the DCC platform.
  - **DCC Marketing Campaign Platform (MCP)** - COD also provides data from the DDE file to the DCC MCP for the purpose of generating Student Aid Report (SAR) transactional emails.
- **Participant Management (PM) system** - COD receives a daily Participant Destination File (which includes IHE identifiers, the program type code, and the award year) from the PM system. The information is used to let the COD system to know who should be granted access to

COD.

- **Debt Management Collection System (DMCS)** - COD receives student grant collections data from the DMCS, and sends a weekly email to FSA staff that reports rejection codes for rejected submissions, how many submissions were received and rejected, and any changes to submissions.
- **Enterprise Data Management Analytics Platform Services (EDMAPS)** - COD sends information to EDMAPS as part of the EDMAPS data collection and management of FSA-related data for operational and analytical purposes.
- **Financial Management System (FMS)** - COD and the FMS exchange summary financial transaction data, acknowledgments, and responses twice daily using automated processes.
- **FSA Cloud** - The FSA Cloud Platform is a hybrid cloud general support system that integrates with the COD system. FSA Cloud specifically:
    - Provides telephony infrastructure for handling call routing for contacts from customers and schools in support of COD, and
    - Communicates with COD for servicer lookup to support calls to the FSA cloud contact centers.
- **NSLDS** - COD and NSLDS share information to support the Direct Loan, Grant, TEACH, and summary level information for Perkins as part of FSA's title IV aid programs. In addition, COD also provides loan and TEACH Exit Counseling as well as IDR application information. NSLDS in turn sends to COD information regarding student eligibility, loans, servicer information, aid applicant and recipient default data, and information to support the evaluation process for the subsidized usage limit regulation. NSLDS also distributes Cohort Default Rates to COD on a weekly basis to support rules in COD for single-disbursement benefits to eligible schools, as well as Closed School Enrollment files.
- **FSA Partner Connect (PPO)** - PPO is a front-end platform for school partners, financial institution partners, FSA staff, and contractors involved in the administration of title IV financial aid for postsecondary education. COD shares IHE-related information with PPO.
- **Postsecondary Education Participants System (PEPS)** - COD receives general eligibility information about all IHEs participating in the Direct Loan or Pell Programs on a daily basis from PEPS. Information from PEPS is IHE-level, not individual-level, and does not contain PII.
- **Oracle Service Cloud (OSC)** - OSC is a SaaS CRM application that supports the COD call centers with their customer service operations for COD Support (school services). OSC has both inbound and outbound

connections with COD Web services to support customer service operations.

- **OIG** - The Office of Inspector General (OIG) interfaces with COD for multiple data transfers including a monthly extract of Master Promissory Note, Master Promissory Note Reference, and Master Promissory Note Event data. Three data files are delivered to OIG on a monthly basis. The SAIG mailbox is used for the delivery and retrieval of files.

External partner systems:

- **Loan Servicers**

  The COD system distributes booked Direct Loan (DL) and TEACH Grant activity to the loan servicers. The loan servicers maintain aid recipient information sent by the COD system for DL Subsidized, DL Unsubsidized, DL PLUS Direct Loans, and TEACH Grants in order to service the aid. COD and the loan servicers exchange data through the SAIG system. Each processing day COD sends a Loan Activity File to each loan servicer. The loan servicers send back a Receipt and Response file after processing. The Receipt is sent by the servicers to acknowledge the Request file was sent. The Response file is sent by the servicers in response to COD's Request. The Response file includes whether the servicer accepted or rejected each record sent.

  - The COD system sends IDR and consolidation application information to loan services for each processing day. COD sends back a Receipt and Response after processing.
- **Equifax & TransUnion** - The COD system interfaces with two credit bureaus: Equifax and TransUnion. COD sends requests to each bureau based on business rules for each aid applicant and recipient or parent of an aid applicant and recipient requiring a credit check. These calls are part of business process flows that are part of COD processing including Direct Loan PLUS loans triggered by COD batch processing and COD Web.

All these interfaces are provided through the SAIG except for DCC, which is transmitted from studentaid.gov to COD using secure transmissions over the internet.

The systems described above obtain records directly from individuals or from IHEs. For Direct Loan PLUS loans, COD also receives credit check information from credit bureaus. Additionally, since COD serves as the system for storing paper files submitted via DCC, COD may obtain PII directly from individuals in the form of paper applications that are scanned and uploaded into COD.

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.gov for aid applicant and recipient interactions (via DCC)
- Phone calls, chats, and other forms of school correspondence with CSRs (via DCC)
- 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 provided by source systems is validated by those systems. PII obtained through recipient-initiated communication with CSRs is validated by aid recipients and internal databases within FSA systems such as CPS and EDMAPS, which interface with COD. In order to validate information stored within other FSA systems, responses are received after each data exchange; responses can include rejections related to unmatched PII.

Information is also verified through data exchange with external databases such as:

- Credit bureaus
- Loan servicers
- IHEs

Verification with these external databases is completed electronically. Responses are received after each data exchange. Responses can include rejections to unmatched PII. Information is verified to ensure the person is the correct aid applicant or recipient.

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

COD uses PII submitted by aid applicants or recipients and schools to determine eligibility for receiving title IV funds from the Department. The COD system performs validation using PII to book loans and account for awarded grants. Booked loans are

[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.

those that are linked to a promissory note submitted by the aid recipient and have an actual, fudned disbursement. Booked awards are transmitted to servicing partners for servicing. Further, PII on booked loans and awarded grants are used to reconcile aid award disbursements with records submitted by IHEs. This information is used to ensure IHEs receive the appropriate amount of financial aid funding for their recipients.

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

No

3.7.1. 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 used to match aid applicant and recipient records contained in COD against records contained in other FSA systems, records maintained by IHEs, and records maintained by other external partners. SSNs are unique identifiers for individuals that remain consistent across all of these systems.

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

□ N/A

Alternatives to using SSNs were considered but determined not to be feasible given the desgn of FSA and partner systems, as well as the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA's data exchanges internally and externally rely on SSN to identify and track

Federal student aid applications across different systems within and outside of the Department.

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, etc.)? If notice is not provided, explain why not.

COD interfaces to receive, maintain, process, and disseminate information with the FSA systems listed in question 3.3. For how those systems provide notice to the public, please refer to each system's PIA, located at https://www2.ed.gov/notices/pia/index.html.

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

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, as COD receives information from other FSA systems. 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

The OIG interfaces with COD for multiple data transfers including a monthly extract of Master Promissory Note, Master Promissory Note Reference, and Master Promissory Note Event data. Three data files are delivered to OIG on a monthly basis. The SAIG mailbox is used for the delivery and retrieval of files. The PII included in the files includes name, SSN, address, and DOB.

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

□ N/A

PII is provided to the OIG to assist investigators in conducting criminal and civil investigations and to assist auditors in performing audits for the overall purpose of detecting and preventing fraud, waste, and abuse in Department programs.

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 may share information (aid applicant's and recipient's name, SSN, DOB, address, or phone number with IHEs, financial institutions, third-party servicers, software vendors and print services for the purposes lised in question 5.6.

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

□ N/A

COD may share information (aid applicant's and recipient's name, SSN, DOB, address, or phone number with IHEs, financial institutions, and third-party servicers for the purposes below:

[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.

- To assist with the determination of program eligibility and benefits.
- To maintain 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 identify whether an aid recipient may have received title IV, HEA program funds at more than one institution of higher education for the same enrollment period in violation of title IV, HEA regulations.
- To identify whether an aid recipient may have exceeded the award limits under title IV, HEA program funds in violation of title IV, HEA regulations.
- To enable IHEs to reconcile, on an aggregate and recipient-level basis, the amount of title IV, HEA program funds that an institution received with the disbursements it made to, or on behalf of, eligible students (including reconciling verification codes, reconciling the funds received with disbursements made by type of funds received, and making necessary corrections and adjustments).
- To enable an institution of higher education to request online credit checks of aid applicants, aid recipients, or endorsers as part of the process for determining the eligibility of aid applicants and recipients for a title IV, HEA Federal Direct PLUS Loan.
- To support the investigation of possible fraud and abuse and to detect and prevent fraud and abuse in title IV, HEA program funds.
- To assist institutions of higher education with student loan default prevention, disclosures may be made to institutions of higher education as to whether an aid applicant or recipient has completed required counseling in the Direct Loan or TEACH Grant programs.

In addition, COD may share information for the following purposes:

- To assist individuals, institutions of higher education, third-party servicers, or software vendors with questions about title IV, HEA program funds, disclosures may be made to institutions of higher education, software vendors, third-party servicers, and Federal, State, or local agencies.
- To assist the Department in determining eligibility for a Federal Direct PLUS Loan, disclosures may be made to consumer reporting agencies.
- To assist individuals, institutions of higher education, third-party servicers, or software vendors with questions about title IV, HEA program funds, disclosures may be made to institutions of higher education, software vendors, third-party servicers, and Federal, State, or local agencies.

COD also shares aid applicant and recipient name and address with the paper correspondence vendor that prints and mails letters to aid applicants and recipients.

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 is shared through secure encrypted transmission. External users (e.g., IHE financial aid officers, loan servicers) access Department systems using a username and password through AIMS. COD sends and receives files through Secure File Transfer Protocol (SFTP) with external entities. This communication is encrypted through SFTP and uses Secure Shell (SSH) encryption to send files from one system to another.

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?

If an individual wishes to gain access to a record in this system, they must contact the system manager at the address listed in the SORN referenced above. They must provide necessary particulars of name, DOB, SSN, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. Requests by an individual for access to a record must meet the requirements in 34 CFR 5b.5.

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

If an individual wishes to amend the content of their personal record within the system of records, they must contact the system manager at the address listed in the SORN referenced above. They must provide name, DOB, and SSN. Individuals must identify the specific items to be changed and provide a written justification for the change. Requests to amend a record must meet the requirements 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 back-end systems' PIAs, and through the SORN 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 COD personnel and contractors responsible for administering COD . Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing COD.

Physical access to the sites of the Department's contractors where this is maintained is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge.

In accordance with the Department's Administrative Communications System Directive entitled "Contractor Employee Personnel Security Screenings," all contract and Department personnel who have facility access and system access must undergo a security clearance investigation. Individuals requiring access to Privacy Act records 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, contractors and Department employees are required to complete security awareness training on an annual basis. Annual security awareness training is required to ensure that contractors and Department users are appropriately trained in safeguarding data.

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. The Department's Information Security and Privacy Policy requires the enforcement of a complex password policy. 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.

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

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.

COD 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. COD 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. COD 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.

Auditing and Accountability.

7.8. 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, COD 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. COD also participates in the OSA and continuous monitoring program. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as computer matching agreements, information sharing agreements, and memoranda of understanding.

7.9. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

7.10. What are the privacy risks associated with this system and how are those risks mitigated?

The main 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 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, limiting users to those who are screened, utilizing least privilege principles, masking SSNs, and encrypting data in transmission. 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 and updating devices' operating software. 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.