Privacy Impact Assessment

For: Common Origination and Disbursement (COD)

Date: May 20 2016

Point of Contact: Cindy Eckley

System Owner: Diana O’Hara

Author: Niki Moore (Alt ISSO)

Office of Federal Student Aid

U.S. Department of Education
1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions. Indicate whether the system is new or existing, and whether or not the PIA is new or being updated from a previous version; specify whether the system is ‘agency’ or ‘contractor.

Common Origination and Disbursement (COD) is an existing, agency owned, contractor run system; this PIA is being updated from a previous version, dated February 3rd, 2005.

The 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 for the following financial aid programs:

- Pell Grant
- William D. Ford Federal Direct Loan
- Perkins Loan
- Academic Competitiveness Grant (ACG)
- National Science and Mathematics Access to Retain Talent Grant (National SMART)
- Teacher Education Assistance for College and Higher Education Grant (TEACH)
- Iraq Afghanistan Service Grants (IASG)

The COD system 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. In addition, COD provides FSA with the following benefits and functionality:

- Streamlines and simplifies the aid origination and disbursement process
- Improves information accuracy by providing a central repository for FSA’s data storage
- Provides integrated customer service
- Transmits via batch or real-time updates
- Provides program integrity through data integration
- Provides one process and record for submitting origination and disbursement data
- Provides edits that are common across programs
- Provides data tags that are common across programs and (approaching) a cross-industry standard for data definitions
- Eliminates duplicate data reporting for Pell, ACG, IASG, National SMART and TEACH Grants and Direct Loans and Perkins Loans
- Streamlines edits to reduce turnaround time for exception processing
- Expands on-line capability to make corrections/changes, process “emergency” requests, and check transmission status
- Provides reporting capabilities to benchmark similar school groups

2. **Legal Authority.** Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

- The Higher Education Act of 1965 (HEA), As Amended, Section 441 and 461 Title IV, Section 401
- Federal Information Security Management Act of 2002
• Computer Security Act of 1987, 44 U.S.C. 3504
• Paperwork Reduction Act, 44 U.S.C. Chapters 29 and 35
• Freedom of Information Act (FOIA), as amended, 5 U.S.C. 552
• Privacy Act of 1974, 5 U.S.C. 552a
• Trade Secrets Act
• Federal Records Act of 1950, as amended, 44 U.S.C. 2901
• Authority: Executive Branch Directives
• OMB Circular A-130, Management of Federal Information Resources
• Homeland Security Presidential Directive 7
• Presidential Decision Directive 67 (PDD 67)
• Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008)

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

The COD system receives, processes and stores privacy act related data, such as names, social security numbers, current address, date of birth, place of birth, telephone numbers, and dollar amounts.

The general public does not have access to COD.

The information is provided by the student applicants and the schools participating in the Title IV Higher Education Student Financial Aid Programs to enable the administration of the Federal Title IV grants and loans by the Department. The Title IV loans and grants are used by eligible students to attend those schools.

4. **Why is the information collected?** How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

FSA/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.

The information contained in this system is maintained for the following purposes related to students and borrowers:

1. To determine recipient eligibility and benefits for Federal grant or loan programs;
2. To store electronic data that support the existence of a legal obligation to repay funds disbursed under Federal grant or loan programs;
3. To identify whether an individual may have received a Federal grant or loan at more than one educational institution for the same enrollment period in violation of program regulations; and
4. To identify whether an individual may have exceeded the annual award limits under the Federal grant or loan programs in violation of program regulations.

Also collected for the following purposes related to students and borrowers:

1. To enable an educational institution 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; 
(2) to enable an institution of higher education to perform on-line credit checks to determine the credit 
worthiness of a borrower for Federal Loans; and 
(3) to assist an institution of higher education, a software vendor, or a third-party servicer with questions 
about a Federal grant or loan.

The information in this system is also maintained for the following purposes relating to the 
Department’s oversight of the Federal grant or loan programs: 
(1) To support the investigation of possible fraud and abuse and to detect and prevent fraud and abuse in 
the Federal grant and loan programs; 
(2) to confirm that an institution of higher education, or a program offered by an institution of higher 
education, is eligible to receive program funds; 
(3) to set and adjust program funding authorization levels for each institution; 
(4) to enforce institutional compliance with Department reporting deadlines; and 
(5) to apply appropriate funding controls.

Protecting the privacy of individuals and their PII that is collected, used, maintained, shared, and 
disposed of by programs and information systems, is a fundamental responsibility of federal 
organizations. Privacy also involves each individual’s right to decide when and whether to share 
personal information, how much information to share, and the particular circumstances under which that 
information can be shared.

The information contained in this system is protected from unauthorized disclosure through the 
implementation of applicable Privacy controls as identified within NIST SP 800-53 Rev 4.

5. Social Security Number (SSN). If an SSN is collected and used, describe the purpose of the 
collection, the type of use, and any disclosures. Also specify any alternatives that you considered, 
and why the alternative was not selected. If system collects SSN, the PIA will require a signature 
by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The SSN is the unique identifier for Title IV student financial assistance programs and its use 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. Trading partners 
include the Department of Education, Internal Revenue Service, Department of Homeland Security, 
Selective Service System, institutions of higher education, national credit bureaus, lenders, and servicers.

FSA/COD uses SSNs to verify identity and retrieve records in coordination with loans, account for 
awarded grants and to enable the Department to reconcile school cash drawdowns from the Treasury to 
individual student disbursements.

This information also is used to ensure the respective schools receive the appropriate amount of financial 
aid dollars for their students during the respective time periods.

The Department of Education asks individuals to supply information to be used in the COD System and 
provides the individual with a written “Privacy Act statement” that can be retained by the individual.

Regulations governing the Federal student financial aid programs require schools to collect and confirm 
the SSN of student borrowers and grantees prior to disbursement of funds. Each time the Department of 
Education asks individuals to supply information to be used in the COD System, the System Manager 
provides the individual with a written “Privacy Act statement” that can be retained by the individual.
This Privacy Act statement informs the individual of the legal authority for collecting the information; whether disclosure of such information by the individual is mandatory or voluntary; the principal purpose(s) for which the information is being collected and the routine uses which may be made of the information; and the effect on the individual if the individual does not provide the information.

6. Uses of the Information. What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The COD system 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.

FSA/COD uses student-level PII as the unique identifier across all interfacing systems 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 also is used to ensure the respective schools receive the appropriate amount of financial aid dollars for their students during the respective time periods.

7. Internal Sharing and Disclosure. With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

Interfacing ED systems are operated for the most part within FSA’s Virtual Data Center (VDC), located in Plano, TX which provides the respective security controls. The COD data is encrypted as it moves between COD system interfaces.

Central Processing System (CPS) is a mainframe application that edits the Free Application for Federal Student Aid (FAFSA) application data and performs matches against Immigration and Naturalization Service (INS), Social Security Administration (SSA), Department of Justice, Selective Service, and National Student Loan Database System (NSLDS) data to determine student eligibility. CPS sends confirmation forms to schools (the ISIR) and students (the SAR).

COD and Debt Management & Collection System (DMCS) will communicate when a file transmitted from DMCS to COD is corrupt to the point of unreadable by the COD system. COD also communicates by sending to DMCS a weekly email that contains award year specific processing files. DMCS will review the files and have the ability to submit an Operations Maintenance Request (OMR) to COD for those transactions that have been rejected by COD.

Student Aid Internet Gateway (SAIG) interface enables Enterprise Service Bus (ESB) to retrieve a batch of Legacy and Common Record Format Record files (including SAIG batch headers and trailers) from SAIG mailboxes periodically throughout the day. The message types included in this interface include Pell/DL Sub and Unsub/DL PLUS/DL Change Originations and Pell/DL Disbursements and ACG, SMART, IASG, TEACH and PERKINS records. The ESB does not need to transform any fields in these files and simply transports them (including the SAIG Header and Trailer Information) to COD for processing.

Participation Management (PM) provides a differential file every two hours to update COD access information.

Access and Identity Management System (AIMS) provides a web service to authenticate COD users. Direct Loan web will retrieve data that is stored outside of the DB2 RDBMS via packet calls to COD.
Postsecondary Education Participants System (PEPS) maintains eligibility, certification, demographic, financial, review, and audit and default rate on all Schools, Lenders and Guarantors participating in Title IV programs. PEPS sends information on school eligibility for financial aid to COD. Online access to the PEPS database is available to individuals from the U.S. Department of Education, Guaranty Agencies (GAs), State Licensing Agencies, Accrediting Agencies, State Departments of Education and other entities with student financial aid oversight roles.

An Oracle Federal Financials suite of applications for financial management functions within the modernization initiative, Financial Management System (FMS) acts as the general ledger for FSA and pays disbursements to schools.

NSLDS is a national database of loans and the financial aid disbursed to students under Title IV of the Higher Education Act of 1964.

Virtual Data Center (VDC) ESB acts as a bridge between the FSA legacy systems and the COD processing system.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

COD / Enterprise Data Warehouse and Analytics (COD/EDW&A) has an interconnection with the U.S. Department of Housing and Urban Development (HUD), Office of Policy Development and Research (PD&R). The purpose of the exchange is to link housing subsidy data with student aid data. HUD transmits sensitive personally identifiable information (PII) data about tenants to include names, dates of birth and social security numbers. Transmission is executed via a Secure File Transfer Protocol (SFTP). The U. S. Department of Education (ED) compares this data against data in COD/EDW&A and returns summary output files and table of percentages that show FASFA submission, type of aid and enrollment in post-secondary institution of higher education within HUD-assisted households. ED will share back with HUD aggregated results that will not transmit or contain sensitive PII.

A Memorandum of Understanding (MOU) between FSA, ED and PD&R, HUD has been signed and dated April 19, 2016. An Interconnection Agreement (ISA) between FSA COD/EDW&A and HUD has been signed and dated April 19, 2016.

Outside of the current MOU/ISA, the information is not usually shared, although it may be made available for a civil or criminal law enforcement activity that is authorized by law, upon a written request by the agency, and other such uses detailed in the relevant System of Records Notice, cited below.

9. **Notice.** Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Extensive Privacy Act notices are posted at the web site of the Free Application for Federal Student Aid (https://fafsa.ed.gov). The basis for the data sent to COD by colleges / universities is the FAFSA, which is filled out by student applicants first. The FAFSA is an OMB approved data collection instrument (OMB #1845-0001).
10. Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.

- http://www.cod.ed.gov (port 80 redirect to port 443)
- https://cod.ed.gov/
- https://studentloans.gov
- https://teach-ats.ed.gov/

11. Security. What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

All information is protected by a PIN or password and is monitored by automated and manual controls. COD, Studentloans.gov and Agreement to Serve websites are developed and maintained under a contract with Accenture, and is housed within a secure facility run under a subcontract with TSYS Inc., one of the largest credit card processors in the world.

The TSYS facility issues identification badges and access cards to individuals who are authorized to access the facility for work related to the COD contract.

Interfacing ED systems are operated for the most part within FSA’s Virtual Data Center (VDC), located in Plano, TX which provides the respective security controls for those systems. The COD data is encrypted as it moves between COD system interfaces.

COD System administrators outside of the VDC provide comparable security controls to protect the system and the information contained therein.

In accordance with FISMA, every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of implemented security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. COD received its ATO on 08/14/2014.

COD security controls are governed by the regulations and standards listed below:

- Federal Information Control Audit Manual (FISCAM)
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- NIST SP 800-35 Guide to Information Technology Security Services, October 2003
12. **Privacy Act System of Records.** Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already
exists, what is the SORN Number?


13. Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

N1-441-09-23