Privacy Impact Assessment

For

Education’s Central Automated Processing System (EDCAPS)

Date:

August 11, 2016

Point of Contact:

D’Mekka Thompson, DMekka.Thompson@ed.gov, (202) 245-7217

System Owner:

Greg Robison, Greg.Robison@ed.gov, (202) 245-7187

Author:

D’Mekka Thompson, DMekka.Thompson@ed.gov, (202) 245-7217

Office of the Chief Information Officer

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.

This is an update of the EDCAPS 2014 PIA. This document is being updated to include the new EDCAPS System of Record Notice (SORN) information and to update the Social Security Numbers (SSNs) Section for the G5 system as EDCAPS no longer supports NIDRR.

Education’s Central Automated Processing System (EDCAPS) is the system that maintains financial and management records associated with the operation of the Department of Education. EDCAPS consists of four major components: Contracts and Purchasing Support System (CPSS II), Financial Management Support System (FMSS), e2 Travel Management System and Grants Management System (G5). The records found within these subsystems are used to prepare financial statements and reconcile general ledger balances with subsystems maintained in program areas, manage funds, process grants and contracts, manage receivables, costs, and recipients, and perform administrative processes (e.g., purchasing, travel, and miscellaneous payments).

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?


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?

PII received into the EDCAPS system comes from various sources including banks, educational institutions, businesses, other federal agencies, and individual users. Records in this system contain individual name and address, telephone number, Taxpayer Identification Number (TIN), Social Security number (SSN), date of birth, e-mail address, banking information, and grant management data, including application and close-out information. Documents maintained in the system include, but are not limited to, activity logs, copies of checks, contracts, court orders, letter of notice, promissory notes, telephone logs, and related correspondence. This information is exchanged within EDCAPS systems.

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.

The purpose of EDCAPS is to maintain financial and management records associated with the fiscal operations of the Department of Education and other entities with contracting authority that use EDCAPS. The PII is collected to carry out the functionalities discussed below.

The main privacy risk identified is the unauthorized access to the PII contained in EDCAPS. This risk has been mitigated through privacy training for both contractor and Department staff, restricting access to PII to individuals with a direct business need for the information, and robust security controls, detailed below in Question 11.

The EDCAPS financial management system consists of a suite of applications including:

**Financial Management Support System (FMSS)**

The FMSS module of EDCAPS is the Department's official general ledger. It is the central piece of the Department's integrated financial management system. FMSS includes functionality for budget planning and execution, funds control, receipt management, administrative payment management, loan servicing, and internal and external reporting. FMSS interfaces with a variety of other EDCAPS systems such as the Grant Management System (G5), Contracts and Purchasing Support System (CPSS II), and Travel Management System (TMS).

**Grant Management System (G5)**

The purpose of G5 is to administer grant awards, from planning through closeout, including disbursing funds to grant recipients for certain Department programs. G5 records individual payments in real time, and summary payment data is posted to FMSS in a nightly batching process. G5 maintains a record of grant awards by the Department, including management information collected during the award process. Payment information is retrievable in G5 by DUNS number; which are unique numbers that are used by businesses and the Federal Government to keep track of more than 70 million organizations worldwide. The name, mailing address and other characteristic data related to Federal grants or institutional loans are also maintained. There are rare occasions when an individual is not eligible for a DUNS, and an SSN is used for grant processing. To mitigate privacy risks, users outside the internal functional team and the individuals themselves have no access to PII. Banking information is accessible to the banking team only. Reports are carefully designed to suppress the PII. Access to production and reporting database is by authorized users. Strict instructions are provided to not extract or share PII data without proper handling and authorization.

**Contract and Purchasing Support System I and II**

CPSS II is replacing CPSS I. CPSS supports the pre-award and post-award processes for all types of contracts, delivery orders, task orders, interagency agreements, small purchases and purchase card transactions. Requirements can be consolidated at any level and multiple awards may be made from a single requirement. Awards are modified financially or administratively as necessary, until closed in CPSS. CPSS interfaces with FMSS in real time at the detail level for funds check, commitments, and obligations. Information is exchanged for vendors, accounting codes, and purchase card payment files. Financial transactions involve a combination of procurement and sub-procurement lines, single and multi-line accounting, and incremental funding where adjustments are required throughout the lifecycle (e.g., adjust commit until
Privacy Impact Assessment

obligate without restriction). Data is exchanged to meet all regulated Government reporting requirements such as system to system integration with the Federal Procurement Data System – Next Generation (FPDS-NG), Central contractor registration (CCR), which is now titled System for Award Management (SAM) and FedbizOpps (FBO).

Travel Management System (TMS)

The Department of Education utilizes the E2 Solutions web-based travel management system (owned and operated by CW Government Travel, Inc.). The TMS collects the traveler’s name, address, e-mail address, and the last 4 digits of the traveler’s Social Security Number. Information is collected in order to authenticate the user, complete official government business on behalf of the individual submitting the information, and to facilitate reimbursing individuals for completing official government travel.

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. If no SSN is collected, no signature is required.

Financial Management Support Systems

The FMSS collects SSNs for processing payments to internal employees (categorized as a payee). SSNs are masked within the system and are not exposed to any users who do not have Administrator privileges. The SSNs are also used for 1099 processing by the FMSS system if an honorarium payment is made to an individual.

Grant Management System

In general, G5 requires DUNS and Bradstreet numbers for grant recipients, however there are rare occasions when individuals are not eligible for DUNS and have to use their SSNs for G5 processing.

Contract and Purchasing Support System I and II

CPSS collects SSNs for processing payments to internal employees (categorized as a payee) who travel for official business, or receive honorariums. The SSN is used as the TIN (Tax Identifier Number) only to properly identify the individual in the contract system and is passed to the financial system though an internal interface. SSNs are masked within the system and are not exposed to any users who do not have Administrator privileges. The SSNs are also used for 1099 processing by the FMSS system if an honorarium payment is made to an individual. This is IRS required data and as such, this information must be used to track payments and issue 1099s. There is no other information used by the IRS. It is used for identification, not authentication. If an individual chose to request a separate TIN from the IRS, that could be used. However, the IRS does not require that. The IRS accepts only TINs, or for individuals, SSNs in place of TINs.

Travel Management Systems (TMS)

TMS collects the last four digits of users SSN for authentication purposes. Other authentication methods were considered, however, the IDs have to be authenticated on information maintained in the financial system, thus the use of the last four numbers of the SSN. There is no feasible alternative.

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 information collected by EDCAPS will primarily be used for

- Accounting for goods and services provided and received
- Enforcing eligibility requirements and conditions in awards and U.S. law relating to transactions covered by this system
- Defending the Department in actions relating to transactions covered by this system
- Investigating complaints
- Updating information
- Correcting errors and investigating fraud
- Performing the receivables management function
- Preparing financial statements and other financial documents.

Each application uses the PII collected for additional specific uses as detailed below:

**Financial Management Support Systems**

Administrative Payments - PII is collected from CPSS to facilitate on behalf of the entity or individual submitting the information to receive payment from Education. Information, such as addresses, phone numbers, taxpayer identification numbers, social security numbers and banking information, is available internally to Department of Education banking staff to review, but is not shared with outside sources except the Department of Treasury for execution of the payments.

Payroll Information – PII is also collected for payroll purposes. The payroll information is shared with the Department of Interior as the Department’s payroll system provider and includes addresses, phone numbers, social security numbers and banking information.

Debt Collections – PII, including taxpayer identification numbers and social security numbers, is collected for Debt Collection. The delinquent debt is sent to Treasury for the purpose of collecting the debt on behalf of the Department.

**Grant Management System**

PII, including date of birth, name, address, phone and email address, is collected in a user registration and external/internal access form. SSNs are collected only for a very few active payees and the SSN is collected in an external user access form. TINs are collected from the SAM interface from GSA and/or PEPS interface from FSA. The information that is collected is used to administer and manage grant awards and disburse funds.

**Contract and Purchasing Support System I and II**

CPSS information will be used for administering the procurement and contracting system of record for processing and issuing contractual commitments and obligations to external entities and to internal employees (categorized as a payee) who travel for official business, or receive honorariums. CPSS receives vendor data from GSA’s System for Award Management (SAM). The CPSS system has built in reports and tools that allow for both recurring and ad hoc data reporting, review, and analysis.

**Travel Management Systems (TMS)**
TMS has been integrated with ED’s accounting system to provide funds control and improved accounting. The PII collected is used to achieve this purpose. The current software provides electronic workflow to reduce paperwork and manual processes. It also supports EFT and split disbursement payments. TMS is an enterprise wide e-gov travel processing system as mandated by the Federal Travel Regulations. TMS supports the Department’s complete travel process and provides a web based end-to-end electronic integrated solution to ED travelers.

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? The information collected in EDCAPS will be shared with other ED offices only as needed, and for a specific government purpose. The EDCAPS applications share data with each other to administer and manage the programs.

   Additionally, the G5 system provides certain grants data to Education Facts (EDFACTS) and the Grant Electronic Monitoring System (GEMS). The GEMS is used to monitor the grants funded by Office of Post-Secondary Education (OPE) and the Office of Elementary and Secondary Education (OESE). Currently, GEMS is being accessed/used only by internal users.

   The following information is being shared with GEMS application:

   1. Application information such as applicant’s name and address.
   2. Budget information such as budget categories, dates, allotment and allocation amounts.
   3. Financial transaction Information such as obligations, drawdown, etc.
   4. Grantee and payee information such as recipient DUNS/SSN and address.
   5. Administrative actions such as program contacts, supplements, and grant transfers.

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?

   The Department may disclose information contained in the systems of records to external entities listed in Number 12 below, under the routine uses listed. These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act, under a computer matching agreement.

   Information from EDCAPS systems is also shared with the U.S. Department of Treasury to facilitate payment to the individual’s banking institution of choice, and to other parties as required by the Freedom of Information Act (FOIA).

   **Financial Management Support Systems:**

   The FMSS receives employee data from the Department of Interior (DOI) to process payroll data. The FMSS and DOI have an MOU in place for this exchange of data. The FMSS sends vendor payment data to the Department of Treasury to facilitate the payment of invoices to these vendors. The FMSS and Department of Treasury have an MOU in place for payment processing.

   **Contract and Purchasing Support System I and II**
CPSS data is not shared with any external parties. It meets all regulated Government reporting requirements such as system to system integration with the Federal Procurement Data System – Next Generation (FPDS-NG), Central contractor registration (CCR), which is now titled System for Award Management (SAM) and FedbizOpps (FBO). CPSS has MOUs in place for FPDS-NG, GSA SAM, and FedBizOps.

**Travel Management Systems (TMS)**

TMS data is not shared with external parties. The system is covered under a MOU/ISA.

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?

General notice is provided to the individual prior to information collection on the ED.gov Privacy Notice page at: [http://www2.ed.gov/notices/privacy/index.html](http://www2.ed.gov/notices/privacy/index.html)

Individuals have an opportunity to decline to provide information as stated on the website:

“We collect no personal information about you unless you choose to provide that information to us. We do not give, share, sell, or transfer any personal information to a third party. Some of our web pages (such as online publication order forms, conference and training registration forms, web discussion forums) let you voluntarily submit personal information. In those cases, we will provide a specific notice before you begin submitting any personal information, explaining how your information will be safeguarded.”

Individuals consent to the uses of the information by providing the requested information.

Additional notice is provided to grantees whose SSNs are collected on the form that is the point of collection for the Grants Management System.

For CPSS, individuals must provide either an SSN or a Tax ID (TIN) in order to receive payments. This is a required and authorized use. If the individual fails to provide the requested information, they will not receive the payments.

10. **Web Addresses.** List the web addresses (known or planned) that have a Privacy Notice.

    General notice is provided at [http://www2.ed.gov/notices/privacy/index.html](http://www2.ed.gov/notices/privacy/index.html).

    Because none of the systems are open to the general public, additional website privacy notices are not required.

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?

A-130 Appendix III and Public Law 100-235, “Computer Security Act of 1987” is covered by an approved and current system security plan. The system security plan details the security requirements and describes the security controls that are in place to meet the computer security requirements listed above. Furthermore, our security controls are validated by a certification and accreditation process in accordance with the National Institute of Standards & Technology “Guide for the Security Certification and Accreditation of Federal Information Systems.”

A brief summary of the security controls in place is listed below:

- Access to EDCAPS is only available to authenticated users who have a valid system user ID and password and who have logged on to the network.
- Management approves all access and roles and responsibilities.
- The logical boundaries of EDCAPS are protected by a combination of firewalls, intrusion detection systems, and event monitoring systems.
- Every EDCAPS user is provided a copy of the Rules of Behavior prior to accessing the system.
- Passwords comply with a strong password complexity policy.
- EDCAPS servers are housed in environmentally controlled server rooms.
- There are scheduled system audits, user recertification/deprovisioning host and network intrusion detection, and vulnerability scans.
- Users outside the internal functional team and the individuals themselves have no access to the PII information. Banking information is accessible to the banking team only. Reports are carefully designed to suppress the PII information.
- Access to production and reporting database by authorized users only. Strict instructions are provided not extract or share PII data without proper handling and authorization.

12. **Privacy Act System of Records.** Is the information within the system retrieved by personal identifier? 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?

EDCAPS (including the FMSS, G5, and CPSS II subsystems) is covered under System of Records Notice (SORN) 18-03-02, Education’s Central Automated Processing System (EDCAPS), December 24, 2015, Federal Register 80, Number 247, Pages 80331 - 80339. Travel Manager System is covered by General Services Administration (GSA) government-wide SORN entitled "Contracted Travel Services Program" (GSA/GOVT-4) located at [http://www.nsf.gov/policies/SOR_govt-4_contracted_travel.pdf](http://www.nsf.gov/policies/SOR_govt-4_contracted_travel.pdf)

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:

Records relating to Education’s Central Automated Processing System (EDCAPS) are retained in accordance with ED 069 – FSA Financial Management System, and ED 254 – Grant Management System (G5).

In general, all records are retained for various periods of time; however the minimum for all systems is six (6) years, and three (3) months.
Privacy Impact Assessment

Records in the FMSS module are retained in accordance with General Records Schedule (GRS) 7.2. FMSS records are destroyed six (6) years, and three (3) months after the close of the fiscal year in which the records were created. Records in the G5 and CPSS II modules are retained in accordance with GRS 3.3(a)(2)(a). G5 and CPSS II records are destroyed six (6) years and three (3) months after the final payment is made.