



Privacy Impact Assessment (PIA)
for the

Education's Central Automated Processing System (EDCAPS)

October 29, 2019

For PIA Certification Updates Only: This PIA was reviewed on **October 29, 2019** by **D'Mekka Thompson** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: D'Mekka Thompson, EDCAPS ISSO
Contact Email: dmekka.thompson@ed.gov

System Owner

Name/Title: Christopher Shanefelter
Principal Office: Office of the Chief Information Officer (OCIO)

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

Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. **If a question does not apply to your system, please answer with N/A.**

1. Introduction

- 1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

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), 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).

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

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.

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.

Payroll Information – PII is also collected for payroll purposes.

Contract and Purchasing Support System: PII 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.

Travel Management Systems (TMS): The PII collected is used to achieve TMS integration with Department of ED's accounting system to provide funds control and

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](#)

improved accounting.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

1.5. Is the system operated by the agency or by a contractor?

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

N/A

[Click here to select.](#)

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.

Authority for maintenance of the system includes the Budget and Accounting Procedures Act of 1950 (Pub. L. 81-784); Federal Managers' Financial Integrity Act (FMFIA) of 1982 (Pub. L. 97-255); Prompt Payment Act of 1982 (Pub. L. 97-177); Single Audit Act of 1984 (Pub. L. 98-502); Cash Management Improvement Act of 1990 (Pub. L. 101-453); Chief Financial Officers Act of 1990 (Pub. L. 101-576); Government Performance and Results Act (GPRA) of 1993 (Pub. L. 103-62); Federal Financial Management Act (FFMA) of 1994 (Pub. L. 103-356); Federal Financial Management Improvement Act (FFMIA) of 1996 (Pub. L. 104-208); E.O. 013478 (collection of Social Security Numbers); Government Accountability Office Policy and Procedures Manual; Statement of Federal Financial Accounting Standards published by the Government Accountability Office and the Office of Management and Budget; 31 U.S.C. 3701-20E; Federal Claims Collection Act of 1966 (Pub. L. 89-508); Debt Collection Act of 1982 (Pub. L. 97-365); and Debt Collection Improvement Act of 1996 (Section 31001 of Pub. L. 104-134).

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

System of Records Notice (SORN) 18-04-04, Education’s Central Automated Processing System (EDCAPS), December 24, 2015, Federal Register 80, Number 247, Pages 80331 – 80339.

<https://www.federalregister.gov/documents/2015/12/24/2015-32501/privacy-act-of-1974-system-of-records>

Travel Manager System is covered by General Services Administration (GSA) government-wide SORN entitled "Contracted Travel Services Program" (GSA/GOVT-4) located at

<https://www.federalregister.gov/documents/2009/06/03/E9-12951/privacy-act-of-1974-notice-of-updated-systems-of-records>

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

N/A

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.

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>

Records relating to Education's Central Automated Processing System (EDCAPS) are retained in accordance with General Records Schedule disposition authorities below:

Records in the FMSS module are retained in accordance with General Records Schedule disposition authority - GRS 1.1 Item 011 (DAA-GRS-2013-0003-0002)

FMSS disposition is TEMPORARY

Destroy/delete when business use ceases

Records in the G5 module are retained in accordance with General Records Schedule disposition authority- GRS 1.2 Item 020 (DAA-GRS-2013-0008-0001)

G5 disposition is TEMPORARY

Destroy/delete 10 years after file cutoff.

Records in the CPSS module are retained in accordance with General Records Schedule disposition authority- GRS 1.1 Item 011 (DAA-GRS-2013-0003-0002)

CPSS disposition is TEMPORARY

Destroy/delete when business use ceases

Records in the e2 Travel module are retained in accordance with General Records Schedule disposition authority- GRS 1.1 Item 011 (DAA-GRS-2013-0003-0002)

E2Travel disposition is TEMPORARY

Destroy/delete when business use ceases

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

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

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, bank information (i.e. bank account, bank name and routing number), and grant management data (i.e. grant competition information, grant application data,

applicant information (school, project director, legal address, DUNS, school TIN), grant reviewer information (name, resume information, contact information, grant reviewer comments, scores and recommendations, grantee details, including institution DUNS, TIN, address and contacts, financial data, funding and expenditures, performance reports and audit and monitoring artifacts to include 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 stored within encrypted tables on the EDCAPS databases.

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

Yes

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

PII received into the EDCAPS system comes from various sources including banks, educational institutions, businesses, other federal agencies (i.e. Department of Treasury, Department of Interior and GSA), and individual users.

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

G5- Information is collected by paper form for external G5 applicants and bank account forms, electronic forms for G5 internal users and electronic interfaces for FSA's Postsecondary Education Participants System (PEPS) and System for Awards Management (SAM) DUNs that include TINs.

CPSS- Information is collected by electronic form

FMSS- Information is collected by electronic form

TMS- Information is collected by electronic form

- 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?

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.

G5- Manual validation of filled forms, electronic validation for interfaces, tri-annual user account recertification

CPSS- Manual validation of filled forms, tri-annual user account recertification

FMSS- Manual validation of filled forms, tri-annual user account recertification

TMS- Manual validation of filled forms, tri-annual user account recertification

A validation of financial data is conducted annually through the Financial Statement audit which is conducted by a third-party.

Use

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

The information collected by EDCAPS will primarily be used for

- General ledger - Preparation of financial statements and reconciliation of general balances with subsystems maintained in program areas and Treasury
- Funds management - Budget formulation, budget execution, and funds control
- Grants pre- and post-award processing, including grant payment processing
- Contract pre- and post-award processing
- Administrative processes (e.g., purchasing, travel, and miscellaneous payments)
- Serves as the source for all budget funding transactions and establishes budget authority for the Department

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

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 (This is IRS required data and as such, this information must be used to track payments and issue 1099s).

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 through an internal interface. SSNs are masked within the system and are not exposed to any users who do not have Administrator privileges.

TMS collects the last four digits of user's SSN for authentication purposes.

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

N/A

For TMS 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.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The Standard Form 3881 and the IRS W-9 and 1099 forms used by EDCAPS all contain a Privacy Act Statement.

- 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

SF Form 3881: “The following information is provided to comply with the Privacy Act of 1974 (P.L 93-579). All information collected on this form is required under the provisions of 31 U.S.C. 3322 and 31 CFR 210. This information will be used by the Treasury Department to transmit payment data, by electronic means to vendor’s financial institution. Failure to provide the requested information may delay or prevent the receipt of payments through the Automated Clearing House Payment System.”

IRS Form W-9: “Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.

IRS Form 1099: “This notice is given under the Privacy Act of 1974 and the Paperwork Reduction Act of 1995. The Privacy Act and Paperwork Reduction Act requires that the Internal Revenue Service inform businesses and other entities the following when asking for information.

The information on this form will carry out the Internal Revenue laws of the United States. We will comply with Internal Revenue Code (IRC) section 6109 and the regulations hereunder, which generally require the inclusion of an Employer Identification Number (EIN) on certain returns, statements, or other documents filed with the Internal Revenue Service. Information on this form may be used to determine which Federal tax returns are required to file and to provide related forms and publications. This Form will be disclosed to the Social Security Administration for their

use in determining compliance with applicable laws. An EIN will not be issued unless you provide all of the requested information, which applies to your entity.

Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by IRC section 6103.”

- 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?

Individuals have an opportunity to decline to provide information as stated on the forms.

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

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.

- 4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

- 5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

- 5.2. What PII will be shared and with whom?

N/A

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

N/A

[Click here to enter text.](#)

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

The information from the EDCAPS application FMSS is 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). The FMSS sends vendor payment data to the Department of Treasury to facilitate the payment of invoices to these vendors.

FMSS also provides employee data to the Department of Interior (DOI) to process payroll data (this includes addresses, phone numbers, social security numbers and banking information). FMSS and DOI have an MOU in place for this exchange of data.

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

N/A

FMSS collects PII to send vendor payment data to the Department of Treasury to facilitate the payment of invoices to vendors; to send delinquent debt to Department of Treasury for the purpose of collecting the debt on behalf of the Department; and for administrative payments this information is shared with Department of Treasury to execute payments.

FMSS also collects payroll information to send to Department of Interior to process as our payroll system provider.

⁴ If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. 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

This information is shared with the Department of the Treasury using a two way path over TCP using the Connect: Direct Secure Server Proxies (SSP).

The information is shared with the Department of Interior by connecting to DOI via Hypertext Transfer Protocol Secure (HTTPS) connection using a web browser.

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?

System of Records Notice (SORN) 18-04-04, 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 <https://www.federalregister.gov/documents/2009/06/03/E9-12951/privacy-act-of-1974-notice-of-updated-systems-of-records>

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

Please refer to the SORN. Information can be found here:

"<https://www.federalregister.gov/documents/2015/12/24/2015-32501/privacy-act-of-1974-system-of-records>"

"<https://www.federalregister.gov/documents/2009/06/03/E9-12951/privacy-act-of-1974-notice-of-updated-systems-of-records>"

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

Please refer to the SORN. Information can be found here:

"<https://www.federalregister.gov/documents/2015/12/24/2015-32501/privacy-act-of-1974-system-of-records>"

"<https://www.federalregister.gov/documents/2009/06/03/E9-12951/privacy-act-of-1974-notice-of-updated-systems-of-records>"

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 EDCAPS is only available to authenticated users who have a valid system user ID
- 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 that they must acknowledge and sign prior to being granted access to the system.
- Users (with the exception of TMS users who utilize userid/password) must log on with their PIV card)
- 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 PII. Banking information is accessible to the banking team only. Reports are carefully designed to suppress PII.
- Access to production and reporting database by authorized users only. Strict instructions are provided to not extract or share PII data without proper handling and authorization.

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.

OMB Circular A-123 Circular Appendix A (Management's Responsibility for Enterprise Risk Management and Internal Control) defines management's responsibility for internal controls by providing guidance on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal controls. These internal controls (i.e. Security Management, Configuration Management, Segregation of Duties, Contingency Planning, Business Processes, Data Management) are also tested/audited yearly by third-party assessment team under the requirements for FMFIA. Lastly EDCAPS undergoes annual system security authorization to maintain an active authority to operate (ATO). The ATO process includes an assessment of security controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The EDCAPS system applications undergo yearly OMB Circular A-123 Appendix A (Management's Responsibility for Enterprise Risk Management and Internal Control) assessment, Financial Statement audits and NIST 800-53 system security control self-assessments. Vulnerability scans are run weekly on the servers and monthly on the databases hosting the applications to identify any threats or risks to the applications.

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

Yes

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

The 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 those individuals with a direct business need for the information, and robust security controls identified below:

- The logical boundaries of EDCAPS are protected by a combination of firewalls, intrusion detection systems, and event monitoring systems.

- EDCAPS servers are housed in environmentally controlled server rooms. All PII data is suppressed/masked. Least privilege is practiced meaning no user will have access to more than what is needed to complete their duties.