Privacy Impact Assessment (PIA)

for the

Education's Central Automated Processing System (EDCAPS)

February 15, 2022

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: D'Mekka Thompson/Alternate System Owner
Contact Email: dmekka.thompson@ed.gov

System Owner

Name/Title: Christopher Shanefelter/System Owner
Principal Office: Office of Finance and Operations (OFO)

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.

Central Automated Processing System (EDCAPS) is the system that maintains financial and management records associated with the operation of the U.S. Department of Education (Department). EDCAPS consists of four major web applications: Contracts and Purchasing Support System (CPSS), Financial Management Systems Software (FMSS), e2 Travel Management System (TMS), and Grants Management System (G5). The records found within these subsystems are used to prepare financial statements and reconcile general ledger balances with systems 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).

Records are used for, but are not limited to, the following:

- Managing grant and contract awards.
- Making payments to the U.S. Department of the Treasury (Treasury), vendors, and/or grantees.
- Accounting for goods and services provided and received.
- Enforcing eligibility requirements and conditions in awards and Federal laws relating to transactions covered by this system.
- Defending the Department in actions relating to transactions covered by the EDCAPS applications.
- Investigating complaints.
- Correcting errors and investigating financial fraud.
- Performing the account receivables management functions to ensure money is paid by the debtor.
- Preparing financial statements and other financial documents.

The EDCAPS financial management system consists of a suite of four web applications:

a) <u>Financial Management Systems Software (FMSS)</u>

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 financial reporting. FMSS interfaces with other EDCAPS systems including the G5, CPSS, and TMS.

Name, address (business or home), telephone number, Taxpayer Identification Number (TIN), Social Security number (SSN), and bank information (i.e., bank account number, bank name, and routing number) are collected from CPSS to facilitate administrative payments to entities or individuals and for payroll purposes.

b) Contract and Purchasing Support System (CPSS)

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. Contracts can be consolidated at any level and multiple awards may be made from a single contract. Awards are modified financially or administratively as necessary until closed in CPSS. CPSS submits data electronically to FMSS, in real time, for funds checks, financial commitments, and obligation payments. Information such as accounting codes, and purchase card payment files is submitted for vendors and/or individuals. 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. Data are exchanged to meet all reporting requirements such as system-to-system integration with the Federal Procurement Data System – Next Generation (FPDS-NG) and System for Award Management (SAM).

PII (including SSNs) is collected for processing and issuing contractual commitments and obligations to external entities and to internal employees (categorized as payees) who travel for official business or receive honorariums.

c) Grant Management System (G5)

G5 administers 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 are posted to FMSS nightly. G5 maintains a record of Department grant awards, including management information collected during the award process. Payment information is retrievable in G5 by the Data Universal Numbering System (DUNS) number. Dun and Bradstreet (D&B) is a company that issues DUNS numbers, which are unique numbers that are used by businesses and the Federal Government to keep track of businesses worldwide. Some entities, such as States and universities, will also have what is known as "DUNS + 4," which is used to identify specific units within a larger entity. G5 also maintains grant competition information, grant application data, applicant information (school, project director, legal address, DUNS, school TIN) and other characteristic data such as grant reviewer information (name, resume, contact information, grant reviewer comments, scores and recommendations), and 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 related to Federal grants or institutional loans.

d) Travel Management System (TMS)

The Department utilizes the E2 Solutions web-based TMS (owned and operated by CW Government Travel, Inc.). The TMS collects the traveler's name, address, and email address. Information is collected on behalf of the Department employee or contractor submitting the information and to facilitate reimbursing individuals for completing official government travel. For the purposes of invitational travel,[1] TMS administrators manually provide documents through encrypted to the CPSS team so that the particular individual can be added as an invitational traveler.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] 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 with contracting authority that use EDCAPS.

- FMSS - Administrative Payments: PII is collected from CPSS to facilitate on behalf of the entity or individual submitting the payment request to receive payment from the Department.
- FMSS - Payroll Information: PII is collected for payroll purposes from the U.S. Department of the Interior (DOI). DOI sends the Department a bi-weekly payroll file and is used to create vendor records for both FMSS and TMS as well as to update employee records. The payroll file information the Department receives is used for the Department to setup employees as "Vendors" in FMSS so that the employee can be paid for official travel or honorariums. The DOI interface uses SSN as a primary key.
- G5: PII is collected for grant management in administering grant applications and competitions to educational institutions and/or individual grantees.
- CPSS: PII is collected for administering the procurement and contracting system for processing and issuing contractual commitments and obligations to external entities and to Department employees and contractors (categorized as a payee) who travel for official business or receive honorariums.

[1] In certain circumstances, the Department may authorize official travel for people who are not civilian employees. Such travel is known as invitational travel.

[2] 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

- TMS: PII is collected to provide travel policy controls, funds control, improve accounting, travel related booking and issuance of reservations for Department employees and contractors who complete official travel.

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 required biennial review.

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

Agency

FMSS, CPSS, and G5 are owned and operated by the Department.
TMS is owned and operated by CW Government Travel, Inc. and managed by the Department. OFO Travel team is the system administrators who performs tier 1 helpdesk support and administrative functions. Any issues that can't be resolved in house will be referred to CW Government Travel.

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.

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

The information is retrieved by individual or entity name, SSN, TIN, or DUNS.

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)).[3] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

FMSS, G5, and CPSS are covered by the System of Records Notice (SORN) 18-04-04, Education's Central Automated Processing System (EDCAPS), December 24, 2015, 80 FR 80331 located at: https://www.federalregister.gov/documents/2015/12/24/2015-32501/privacy-act-of-1974-system-of-records

TMS is covered by the General Services Administration (GSA) government-wide SORN entitled "Contracted Travel Services Program" (GSA/GOVT-4), July 9, 2009, 74 FR 26700 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.

[3] 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

☑ N/A

Click here to enter text.

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

Records relating to EDCAPS are retained in accordance with General Records Schedule disposition authorities below:

- *Retention for FMSS, CPSS, and e2 Travel Module*: GRS 1.1, Item 010: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

- *Retention for G5*: Temporary. GRS 1.2, Item 020: Destroy 10 years after final action is taken on file, but longer retention is authorized if required for business use.

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.

FMSS, CPSS, TMS, and G5 all maintain: Individual (payee or grantee) or entity name and address (home or business), telephone number, entity TIN, SSN (with the exception of G5), date of birth, email address, and bank information (i.e., bank account number, bank name, and routing number).

In addition, G5 maintains:

- grant competition information
- grant application data
- applicant information
    - school
    - project director
    - legal address
    - DUNS
    - school TIN
- grant reviewer information
    - name
    - resume
    - contact information
    - grant reviewer comments
    - scores and recommendations
- grantee details
    - institution DUNS
    - TIN
    - physical school address
    - points of contact
    - financial data
    - funding and expenditures
    - performance reports
    - audit and monitoring artifacts

In addition, CPSS maintains information about the contracts and services performed in line-item data and any supporting documents contracting personnel may attach within CPSS.

In addition, TMS maintain travel details, to include travel dates and locations.

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

Yes

EDCAPS collects only the minimum information necessary to achieve the respective purposes of the applications listed below.

- TMS at a minimum requires the following information for system registration: name, date of birth, home address, email address and phone number. In order for the individual to book travel, they must provide their gender (required by TSA), TSA Precheck number (if possessed by the traveler), travel credit card, emergency point of contact information (required).

- G5 requires school DUNS, TIN and banking information to validate the school risk and ensure payments are made to the correct entity.

- 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. CPSS at a minimum requires the following for travelers: name, SSN, address and banking information in order for the traveler to be reimbursed. CPSS requires the following for vendors: name, Employee Identification Number (EIN)/SSN, address, phone number, email address and banking information for payment purposes.

- FMSS at a minimum requires name, SSN, address and banking information from CPSS and DOI interfaces in order to make payments, issue 1099s and record employee payroll amounts in the General Ledger (GL).

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

PII maintained by the EDCAPS system comes from various sources including banks, educational institutions, businesses, other federal agencies (i.e., Treasury, DOI, and GSA), and individual (payee or grantee) users.

- TMS: PII is collected from the individual traveler which would be a Department employee or contractor.

- G5: PII is collected from the school entity.

- CPSS: PII is collected from the Invitational Traveler, Vendor or GSA SAM.

- FMSS: PII is collected from CPSS and DOI.

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: External user access form for payees associated with the grant awards are collected via mail, fax or email. The form contains username, email, phone, school payee DUNS and name, supervisor name and approval signature. We also collect electronic forms for G5 Department users with name, email, office phone and office location. The forms are processed by internal functional G5 staff and stored electronically in secured folders with limited user access. Paper payee forms are destroyed after being scanned and uploaded to the secured folders. Information is collected by paper form (Standard Form 199A) for G5 applicants, electronic forms through the use of SharePoint online workflow for G5 internal users (Departmental employees and contractors). G5 also utilizes electronic interfaces to collect Federal Student Aid's Postsecondary Education Participants System (PEPS) and GSA's System for Awards Management (SAM), which include TINs.

- CPSS: Information is collected by electronic form W-9 (www.irs.gov) and Standard Form 3881. The Internal Revenue Service (IRS) forms submitted by the Principal Offices originate from the vendors themselves.

- FMSS: Information is collected by the Contracts and Acquisition Management (CAM) Waiver form, Accounts Receivable and Bank Management Division (ARBMD) requests (forms are received via email or via a file upload), DOI employee vendor interface, and Contracts and Purchasing Support System (CPSS) vendor interface. Financial Management Support System (FMSS) does not receive any IRS forms; however, the Department does issue the IRS form 1099.

- TMS: Information is collected by electronic submission on the https://e2.gov.cwtsatotravel.com/ website.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

FMSS, CPSS, and G5: PII is directly received from individual payees and or businesses in order to receive payments. The confirmation and integrity of the CPSS and FMSS

[4] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

information is handled outside of the EDCAPS applications. During the annual submission of 1099 reports to the IRS and vendors the Department may receive notices of correction to reported information. Those corrections to PII will be made in CPSS and FMSS accordingly. DOI also provides corrections to employee PII information that will update employee vendor records each pay period as needed. For CPSS vendors that are matched to General Services Administration (GSA) System of Award Management (SAM), daily files are processed to update PII in the CPSS vendor records and those changes are interfaced to FMSS accordingly. For G5, payees are vetted via the external payee access form submitted by the user accompanied by a letter with the school letterhead requesting the access and verified by a school supervisor. Bank accounts are maintained by an independent banking team and no other user can change, add or delete the bank accounts. The payees can request payments, but they can't select preset bank accounts. Banks and payees are tied by the Payee DUNS in G5. The G5 payment team, an independent user group, schedules and certifies payments prior to submitting them to treasury.

TMS: PII is provided and managed by the individual. Individuals have ability to correct any inaccurate information on the submission website.

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:

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

TMS: PII is used to secure and confirm travel reservations, issue travel tickets, reimburse travel expenses incurred during travel, determine traveler's location, and document the date of tour of duty (TDY) destinations. Employee's work and home address is used to determine which city a traveler can fly out from to their destination.

G5: PII is used for grants pre-award processing, to include accounting for the grant application submission and review process. Grant processing encompasses grant award notification, funding, and grant payment processing.

FMSS: PII is used to fulfill the annual filing of 1099s to the IRS and payment requests to Treasury.

CPSS: PII is used to support the vendor interface to FMSS.

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 Form 1099 processing by the FMSS system if an honorarium payment is made to an individual (SSNs are required by the IRS and, as such, this information is 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 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.

TMS collects the last four digits of a user's SSN for authentication purposes and are used as part of the individuals userid. The userid for TMS is authenticated against information maintained in FMSS.

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

☐ N/A

FMSS: Collects SSNs for processing payments and 1099 processing by the FMSS system if an honorarium payment is made to an individual (SSNs are required by the IRS, as such, there is no feasible alternative.)

CPSS: Collects SSNs/TINs for processing payments, this information is used to interface the tax reporting and payment reporting details needed in supplying payment requests to Treasury and annual 1099 reports to the IRS. The SSN/TIN are the only identifiers used by IRS and, as such, there is no feasible alternative.

TMS: Other authentication methods were considered; however, in order to gain access, individuals need to be verified, thus the use of the last four numbers of the SSN in order to verify the individual. This is a GSA requirement in agreement with CW Travel on how User ID's would be established thus 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.

- FMSS: Utilizes the Internal Revenue Service W-9 and 1099 forms, which both contain a Privacy Act Statement.
  CPSS: Utilizes the GSA Standard Form 3881, which contains a Privacy Act Statement.
- G5: Utilizes the GSA Standard Form 1199A, which contains a Privacy Act Statement and the Department of Education G5 Payee Access Request Form.
- TMS: The TMS website contains 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

- FMSS
  - IRS W-9 (https://www.irs.gov/pub/irs-pdf/fw9.pdf)
  - IRS 1099 (https://www.irs.gov/pub/irs-pdf/f1099msc.pdf)
- CPSS: GSA SF 3881 (https://www.gsa.gov/Forms/TrackForm/33015)
- G5
  - GSA SF 1199A (https://www.gsa.gov/Forms/TrackForm/32810)
  - Department of Education G5 Payee Access Request Form

    Authorities: The following authorizes the collection of this information: Federal Funding Accountability and Transparency Act of 2006 (31 U.S.C. 6101 note).

    Information Collected: Payee User name (First, Last, Middle Initial), telephone number, email address, senior officer of grantee institution name, title, and officer telephone number.

    Purpose: The purpose of collecting this information is used to obtain Payee access (ability to draw funds from grant awards) or make changes to an existing Payee account.

    Disclosures: The information will not be disclosed outside of the Office of Finance and Operations.

    Consequences of Failure to Provide information: Failure to provide required information or forego creating an account may result in not gaining Payee access within G5.

    Additional information about this system can be found in the Privacy Impact Assessment.

- TMS: The TMS website contains a Privacy Act Notice.

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 by simply not filling out the required form(s). However, providing certain information is required in order for the proper processing to occur.

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

EDCAPS shares grant, direct loan funding and payment details to FSA. FSA sends EDCAPS institution grantee/payee/recipient DUNS and TIN along with funding details (obligation monetary amounts) and EDCAPS shares back financial transaction details including (payment amounts, payment confirmations, payment returns and refunds). No PII about individuals are shared through this internal sharing.

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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.[5]
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 Treasury to facilitate payment to the individual's banking institution of choice. The FMSS sends vendor payment data to Treasury to facilitate the payment of invoices to these vendors.

FMSS also provides employee data to DOI to process payroll data (this includes addresses, phone numbers, SSNs, and banking information).

G5 provides financial transaction (obligations and expenditures along with the grantee/recipient name) with USA SPENDING as required by the Federal Funding Accountability and Transparency Act of 2006 (FFATA). No PII is shared with USA SPENDING.

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 Treasury to facilitate the payment of invoices to vendors; to send delinquent debt to Treasury for the purpose of collecting the debt on behalf of the Department; and for Treasury to execute administrative payments.

FMSS also collects payroll information to send to DOI to process as our payroll system provider.

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] 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.

The Department is tracking any disclosures to Treasury in regard to payment transactions through the FMSS application. G5, CPSS, and TMS data is transmitted to FMSS, which is then sent to Treasury.

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 Treasury using a two-way path over Transmission Control Protocol (TCP) using the Connect: Direct Secure Server Proxies (SSP).

The information is shared with the DOI by connecting via a 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?

FMSS, CPSS, G5: If an individual wishes to gain access to a record in this system, he or she must contact the system manager listed in the SORN 18-04-04, Education's Central Automated Processing System (EDCAPS), December 24, 2015.

TMS: Each user that has an account on TMS has access to their own account information and what information encompasses their profile. This information is readily available so as long as the user maintains an active account on the application.

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

FMSS, CPSS, G5: If an individual wishes to change the content of a record in the system of records, he or she must contact the system manager listed in the SORN 18-04-04, Education's Central Automated Processing System (EDCAPS), December 24, 2015.

TMS: Each user that has an account on TMS has access to their own account information and can make updates as necessary. This information is readily available so as long as the user maintains an active account on the application.

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

This PIA, as well as the system of records notice listed in question 2.2, details the procedures for correcting information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

EDCAPS is maintained on secure computer servers located in one or more secure Department network server facilities. Access to EDCAPS is limited to authorized contractors and Department employees. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, EDCAPS must receive a signed Authorization to Operate (ATO) from a

designated Department authorizing official. Security and privacy controls implemented by EDCAPS are comprised of a combination of administrative, physical, and technical controls.

All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. In addition, users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

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.

The following tasks are performed to safeguard EDCAPS information:

- Monthly vulnerability scans performed
- Annual contingency plan test performed
- Annual self-assessments conducted; and/or annual security assessments performed by the Department Security AuthorizationTeam
- Annual updates to system security documents
- Annual mandatory Cybersecurity and Privacy Training for employeesand contractors
- Monthly Continuous Monitoring is in place with vulnerability scans (RA-05), hardware/software inventories (CM-08), and configuration management database updates (CM-06) are posted to CSAM.

8. Auditing and Accountability

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

The system owner works with the Department's Privacy Office to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework process to secure an ATO. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document.

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

Yes

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

Privacy risks associated with EDCAPS 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 granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, and encrypting data in transmission (data are shared with Treasury using a two-way path over TCP using SSP and with the DOI by connecting to DOI via HTTPS connection using a web browser). Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.