



Privacy Impact Assessment (PIA)
for the

Education Central Automated Processing System Helpdesk

(EDCAPSHD)

August 2, 2024

Point of Contact

Contact Person: Tom Erdelyi
Title: Information System Owner
Email: Tom.Erdelyi@ed.gov

System Owner

Name: Tom Erdelyi
Title: Information System Owner
Principal Office: Office of Finance and Operations

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

*Please complete this **Privacy Impact Assessment (PIA)**, which describes 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, answer with N/A.*

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**
- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

- 1.1.** Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The Education Central Automated Processing System Helpdesk (EDCAPSHD) is a U.S. Department of Education (Department) system that utilizes the ServiceNow Government Community Cloud (GCC) web-based software-as-a-service (SaaS) application to document and track Education Central Automated Processing System (EDCAPS) support issues and requests. EDCAPS is the system that maintains financial and management records associated with the operation of the Department, and EDCAPSHD is the system used by the helpdesk that supports EDCAPS.

- 1.2.** How does the IT system function to support the project or program as described in Question 1.1?

EDCAPSHD is used by the EDCAPS Customer Support Group (consisting of Department employees and contractors) to open and process trouble tickets. Internal Department users open trouble tickets related to EDCAPSHD supported applications via the Self-Help Portal within EDCAPSHD or by contacting the EDCAPS Customer Support Group via phone or email. External users do not have access to EDCAPSHD; these users open tickets by contacting the EDCAPS customer support group via phone or email. Trouble tickets include questions regarding how to use or access EDCAPS, how to use specific tools within EDCAPS, and account assistance. Examples of requests include assistance with account creation, password reset, finding accounting codes in an EDCAPS application, and general user guidance. All users submitting tickets provide their name, preferred phone number, and preferred email address as contact information. Internal users also provide their principal office and work location.

Once a ticket is received, EDCAPS helpdesk specialists within the customer support group respond to the ticket either by phone or email using the contact information provided by the individual submitting the ticket. Information is retrieved in the system by ticket number.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

<input checked="" type="checkbox"/> Website	<input checked="" type="checkbox"/> Portal	<input checked="" type="checkbox"/> Application
<input type="checkbox"/> Database	<input type="checkbox"/> Server	<input type="checkbox"/> Other (Specify Below)

If you have been directed to “specify below,” describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)¹ is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

PII is collected from Department employees and contractors to provision user accounts in the system to access the system in order to submit trouble tickets.

PII is also collected from any individual that contact the helpdesk (Department employees, contractors, and external users) in order to submit trouble tickets.

This submitted information is used to assist help desk specialists in tracking, remediating, and responding to customers who are experiencing issues with EDCAPSHD supported applications.

Information pertaining to tickets may also be collected for both internal and external users.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor’s role in operating the system.

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](#)

☐ N/A

The contractor manages the FedRAMP-authorized SaaS application hosted by the ServiceNow Government Community Cloud Service Provider (CSP). The contractor's role is to develop and implement system changes, oversee operations, and provide system maintenance as needed.

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

☒ Yes

☐ N/A

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, contact your program attorney.

- 2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

The system is authorized by 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); 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).

System of Records Notice (SORN)

- 2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☐ Yes

☒ No

- 2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

☒ N/A

Records Management

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

- 2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information.

List the schedule(s):

In accordance with General Records Schedule 5.8, disposition authority DAAGRS-2017-0001-0001, records shall be retained for one year. However, EDCAPSHD retains records for a maximum of 4 years to provide historical trends and for audit tracking and resource planning purposes.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

- 3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly

accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Gender or Sex
<input type="checkbox"/> City, State, or County of Birth	<input type="checkbox"/> Country of Birth	<input type="checkbox"/> Home Address
<input checked="" type="checkbox"/> Personal Phone Number	<input checked="" type="checkbox"/> Work Phone Number	<input checked="" type="checkbox"/> Personal Email Address
<input checked="" type="checkbox"/> Work Email Address	<input checked="" type="checkbox"/> Work Address	<input type="checkbox"/> Personal Fax Number
<input type="checkbox"/> Work Fax Number	<input type="checkbox"/> Digital Signature <input type="checkbox"/> Hand Signature	<input type="checkbox"/> Mother's Maiden Name

Other Demographic Information

<input type="checkbox"/> Citizenship and/or Alien Registration Number (A-Number)	<input type="checkbox"/> Military Service	<input type="checkbox"/> Marital Status, Spouse, and/or Child Information (Specify below)
<input type="checkbox"/> Educational Background/Records	<input type="checkbox"/> Group/ Organization Membership	<input type="checkbox"/> Employment Information
<input type="checkbox"/> Physical Characteristics or Biometrics (Height, Weight, etc.)	<input type="checkbox"/> Race/Ethnicity	<input type="checkbox"/> Religion

Identification Numbers

<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Truncated/Partial Social Security Number	<input type="checkbox"/> Driver's License Number
<input type="checkbox"/> Passport Number	<input type="checkbox"/> Employee Identification Number	<input type="checkbox"/> Professional License Number
<input type="checkbox"/> Credit/Debit Card Number	<input type="checkbox"/> Bank/Financial Account Number	<input type="checkbox"/> Personal Device Identifiers/Serial Numbers

<input type="checkbox"/> License Plate Number	<input type="checkbox"/> File/Case ID Number	<input type="checkbox"/> Federal Student Aid Number
<input type="checkbox"/> Student ID Number	<input type="checkbox"/> Student Loan Number	<input checked="" type="checkbox"/> Grant Number
<input type="checkbox"/> Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

<input type="checkbox"/> Username/User ID	<input type="checkbox"/> Password	<input type="checkbox"/> IP Address
<input type="checkbox"/> MAC Address	<input type="checkbox"/> Complaint Information (Specify below)	<input type="checkbox"/> Medical Information (Specify below)
<input type="checkbox"/> Location Data	<input type="checkbox"/> Log Data That Can Be Traced to Individual	<input type="checkbox"/> Photographs of Individuals
<input type="checkbox"/> Videos of Individuals	<input type="checkbox"/> Criminal history	<input type="checkbox"/> Other (Specify below)

If you have been directed to “specify below,” describe the PII: Information pertaining to tickets (i.e., ticket number, grant number) may also be collected for both internal and external users.

- 3.2.** Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees:
Name, work email address, work phone number, principal office,
work location, and information related to tickets.

☒ Federal Contractors

Specify types of information collected from Federal contractors:
Name, work email, work phone number, principal office, work location, and information related to tickets.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State and local government employees), and the types of information collected from each:²

External EDCAPS users (any individual EDCAPS user who is not a Department employee or contractor): Name, phone number, email address, and information related to tickets.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

The sources of PII collected are individuals (internal or external) who have questions or report issues with the affected EDCAPS applications.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, webpage, database)?

PII is collected via the ServiceNow web portal, or via phone or email when an individual calls or emails the helpdesk to report an issue.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

Name, email address, phone number, and ticket number are required to track, remediate, and respond to individuals that have submitted tickets to the helpdesk. Principal office and work location are collected from internal users for tracking issues experienced at different Department locations.

² For example:

From students: name, email address, phone number.

From institution representatives: name, email address, username, password.

Grant number may be included in the ticket if the ticket is related to troubleshooting issues with accessing a grant award.

3.6. Who can access the information maintained in the IT system?

- ☒ Federal Employees
- ☒ Federal Contractors
- ☐ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

The individual who submitted the ticket receives a confirmation email with a ticket number once the question or issue has been logged in the EDCAPSHD system. That email contains the information the individual submitted, allowing them to verify that the information that was collected is valid and correct.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

☐ No

3.8.1. If the above answer to question 3.8 is YES, are you authorized to use PII when such information is used for internal testing, training, and research?

☒ N/A

[Click here to select.](#)

3.8.2. If the above answer to question 3.8 is YES, what controls are in place to minimize the privacy 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.

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

☐ No

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☒ N/A

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☒ N/A

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☒ N/A

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☒ N/A

4. Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

Individuals voluntarily provide information when they contact the helpdesk. Notice of how their information is handled once submitted to the helpdesk is provided through the publication of this PIA.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

☐ No

- 4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☒ N/A

- 4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

Individuals can choose to not provide information to address their EDCAPSHD supported application issue but doing so will prevent help desk specialists from addressing the individual's matter in an efficient and effective manner.

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

N/A

5. Information Sharing and Disclosures

Internal

- 5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

☐ No

- 5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☒ N/A

- 5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☒ N/A

External

- 5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☒ N/A

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☒ N/A

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☒ N/A

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☒ N/A

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☒ N/A

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☒ N/A

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations

on redisclosure and how they are documented and enforced.

☒ N/A

[Click here to select.](#)

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

Internal users have access to a self-help portal where they can submit, view, and track the status of tickets. Both internal and external users can contact the helpdesk to get a ticket created or get an update on an existing ticket that they do not have direct access to within the EDCAPSHD system. Both internal and external users receive an email notification once a ticket has been created to track their issues.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

Internal users can access their information through the ServiceNow web portal and can correct inaccurate or erroneous information. Both internal and external users can call the helpdesk or send an email to correct any inaccurate information contained in a ticket.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

The system sends email summaries of what the individual has provided to the helpdesk as soon as a ticket is created. Contact information for the helpdesk is provided and users can reply to that email to correct their information, or they can call the helpdesk.

7. Safeguards

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

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

☐ Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

☐ Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

☐ Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☒ Low

☐ Moderate

☐ High

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

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), EDCAPSHD must receive a signed ATO from a designated official. FISMA controls implemented are comprised of a combination of management, operational, and technical controls.

Administrative safeguards include completing safeguarding PII training, incident response testing, and training (that includes PII breach actions), and users are required to read and sign the Rules of Behavior (ROB) annually. Media protections (paper and digital) are employed to ensure the control of sensitive data. Additionally, account management and monitoring practices are applied, and configuration changes to the system are tested to ensure there is no impact on the protection of data.

Technical safeguards include using a Department-approved multifactor authentication (MFA) solution, role-based access control (RBAC) is employed to limit access to users with a need-to-know, and sensitive data at rest and in transit are encrypted.

Physical safeguards include monitoring physical access to the facility, access controls for transmission of data, and access control for output devices are provided by a SaaS FedRAMP-authorized CSP.

8. Auditing and Accountability

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

The Information System Owner (ISO) ensures that the information is used in accordance with stated practices in this PIA by completing the Department's Risk Management Framework process to receive an ATO. The ISO ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5 controls are implemented and operating as intended. The NIST controls are comprised of administrative, technical, and physical controls to ensure that information is used in accordance with approved practices. The system owner also participates in all major security and privacy risk briefings and meets regularly with the Information System Security Officer (ISSO).

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

The ISO ensures that the information is used in accordance with stated practices in this PIA through several methods. The first method is by completing the Department's Cybersecurity Risk Management Framework process and receiving an ATO. Additionally, EDCAPSHD participates in the Departments' Ongoing Security Assessment (OSA) process which addresses security and privacy risks throughout the systems' life cycle. The OSA process ensures a variety of security controls are assessed by an independent assessor to ensure the application and the data residing within are appropriately secured and protected. One-third of all security controls are tested each year and the entire system security is re-evaluated every three years.

Additionally, the PIA is reviewed and updated on an as needed basis and at a minimum every two years. These methods together with regular communication with the contractor team and users ensures that the information is used within the stated practices outlined in this PIA.

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

Privacy risks associated with the system include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs. The risks are mitigated by the safeguards detailed throughout the PIA, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans

- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches 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.