Privacy Impact Assessment (PIA)
for the

Education Central Automated Processing System Helpdesk (EDCAPSHD)
April 6, 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: Kelly Cline/Commercial and Federal Management Shared Services Branch Team Lead
Contact Email: Kelly.Cline@ed.gov

System Owner

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

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 Central Automated Processing System (EDCAPS) Helpdesk (HD) is a U.S. Department of Education (Department) organizational instance of the ServiceNow web-based software-as-a-service (SaaS) application that resides on the FedRAMP Government Community Cloud (GCC) platform. EDCAPSHD is used by EDCAPS[1] internal and external customers to open "trouble tickets" and internally by the EDCAPS Customer Support group (consisting of Federal employees and contractors) to respond to these tickets. Trouble tickets include questions regarding how to use or access EDCAPS or how to use specific tools within EDCAPS.

Tickets are submitted through two methods. Internal users can submit tickets through a web portal and both internal and external users can submit tickets via telephone or email. All users submitting tickets provide name, phone number, and email address as contact information to resolve the issue; internal users also provide principal office and work location. Once a ticket is received, the EDCAPS Customer Support group responds to the ticket either by phone or email using the contact information given by the individual submitting the ticket.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected, used, maintained or shared.

PII that is collected and maintained within EDCAPSHD is used to assist help desk specialists in tracking, remediating, and responding to customers who are experiencing issues with EDCAPSHD supported applications.

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

[1] 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).

[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

Currently Operating System

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

New PIA

Guidance on how to apply the definition of PII required that a PIA be completed for the system.

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

Contractor

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); 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?

No

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

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

This information is retrieved through the use of the Cloud Based Helpdesk ticketing system using the incident record number.

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.

The records in EDCAPSHD are covered by the NARA-approved General Records Schedule (GRS) 5.8 Administrative Help Desk Records, disposition authority DAA-GRS-2017-0001-0001, which permits agencies to maintain records for one year unless there is a business need. EDCAPSHD plans to destroy service request tickets no more than four (4) years after the ticket is resolved, or when no longer needed for business use (i.e., ongoing investigations), whichever is appropriate. The Department maintains service request tickets for audit tracking and resource planning purposes and to analyze historical trends.

[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

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.

External customers: First name, last name, phone number and email address are collected from external customers when they call in or send an email to the EDCAPS Helpdesk to create a trouble ticket related to any of the EDCAPSHD supported applications. Information pertaining to incidents related to tickets may also be collected.

Internal customers: First name, last name, work email, work phone number, the name of their principal office, and work location are collected when a trouble ticket related to any of the EDCAPSHD supported applications is created for internal Department customers. Information pertaining to incidents related to tickets may also be collected.

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

Yes

The PII collected and maintained is the minimum amount required by EDCAPSHD to assist help desk specialists in tracking, remediating, and responding to customers who are experiencing issues with EDCAPSHD supported applications.

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

EDCAPSHD supported applications customers who report any issue(s) with the affected application(s).

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

PII is collected when an internal customer submits a trouble ticket via the ServiceNow web portal, or when an internal or external customer either calls or emails the help desk with an issue related to the EDCAPSHD supported applications.

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?

The customer receives a confirmation email with a ticket number once the customer's issue has been logged in the EDCAPSHD system. In that email contains the information the customer submitted, allowing them to verify information that was collected is valid and correct.

Use

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

The Department uses the PII collected by EDCAPSHD to provide technical support activities for EDCAPSHD supported applications. Specifically, the PII is used to assist help desk specialists in responding to internal and external customers who are experiencing issues with the EDCAPSHD supported applications. Technical support activities include the following:

- Managing service requests tickets;
- Assigning work orders;
- Retrieving incident information;
- Troubleshooting;
- Emailing correspondence.

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

[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.

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.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

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

☑ N/A

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.

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

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

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 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.

4.4. 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

If any changes occur to the system related to how information is collected, maintained or used, this PIA will be updated to reflect such changes.

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

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.

No

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

[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.

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☑ N/A

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

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☑ N/A

Click here to select.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

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

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

Internal customers can access their information through the ServiceNow web portal and can correct inaccurate or erroneous information. Both internal and external customers can call the EDCAPSHD agents or send an email to correct any inaccurate information that they see in the automated email they receive once a ticket is logged on their behalf.

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

Question 6.2, above, explains how an individual may correct his or her information once obtained by EDCAPSHD.

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 Authorization 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

Low

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

EDCAPSHD is hosted outside of the Department's network on a FedRAMP-certified Cloud Service Provider (CSP), ServiceNow. The system is provided as a SaaS and is required to complete routine testing of their environment to ensure the confidentially, integrity, and availability of the information in the system and services provided. The CSP enforces security controls over the physical facility where the system is hosted in adherence with FedRAMP standards.

EDCAPSHD utilizes role-based authentication to ensure only authorized users can access information, and they can only access the information needed to perform their duties. All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple access controls. Authentication to the server is permitted only over secure, encrypted connections. A firewall is in place which allows only specific trusted connections to access the data.

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.

EDCAPSHD is a SaaS and is required to complete routine testing of their environment to ensure the confidentially, integrity, and availability of the information in the system and services provided. The CSP enforces security controls over the physical facility where the system is hosted in adherence with FedRAMP standards. ServiceNow performs monitoring, testing, and evaluation of EDCAPSHD.

- As a part of their continuous monitoring plan, ServiceNow evaluates and tests a selection of EDCAPSHD controls internally on a quarterly basis.
- Assessments are conducted annually by ServiceNow as part of FedRAMP continuous monitoring requirement; results are reported within the security assessment report.
- Security documentation is reviewed by the EDCAPSHD Information System Security Officer (ISSO) and the Information System Owner (ISO) annually and updated as required by changes to the system, security posture, or security requirements.
- EDCAPSHD also has a monthly patch management program, and vulnerability scans occur after the monthly patches have been implemented.

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 ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department’s risk management framework process to receive an Authority to Operate (ATO). During the ATO process EDCAPSHD makes sure that the National Institute of Standards and Technology (NIST) 800-53 controls are implemented. The NIST controls comprise of an administrative, technical, and physical controls to ensure that information is used in accordance with approved practices.

The second method is by ensuring that the system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO to ensure the EDCAPSHD administrator or authorized delegate completes reviews system accounts to ensure only authorized individuals have access to system data.

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 EDCAPSHD include unencrypted data being lost, stolen, or compromised or the potential unauthorized access to the PII contained within the system. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include compromise of credentials or embarrassment. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

EDCAPSHD has several privacy risk mitigation strategies in place. 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. 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. In addition, privacy training is provided for both contractor(s) and Department staff.