Privacy Impact Assessment (PIA)
for the

Electronic Cohort Default Rate (eCDR) Appeals System

Feb 27, 2019

This PIA was originally approved on Dec 7, 2007 and reviewed on Feb 15, 2019 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Fernando Felixberto

Contact Email: Fernado.Felixberto@ed.gov

System Owner

Name/Title: Monica Williams

Program Office: Federal Student Aid (FSA)

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.***

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 Describe the system including the system name, system acronym, and a brief description of the major functions.

The Electronic Cohort Default Rate Appeals (eCDRA) System is an existing Major Application (MA) within FSA's ITA infrastructure. The Department of Eduction Calculates "cohort default rates" for schools that participate in the Federal Family Education loan (FFEL) and the William D. Ford Federal Direct Loan (Direct Loan) programs. This cohort default rate forms an important basis for a school's eligibility to continue participating in the federal student aid programs. The Department releases cohort default rates twice each year. After receiving their cohort default rates, schools have an opportunity to challenge their draft cohort default rates and/or appeal their official cohort default rates, based on an number of circumstances. These challenges involve the exchange of information between the Department and the school that invokes its right to challenge/ appeal. Additionally, Data Managers (guaranty agencies or loan servicers) must in some cases opine on school's request and/or provide supporting evidence for or against the school's challenge/appeal. The system is a Java Enterprise Edition (JEE) web-based application that facilitates the exchange of information between parties for four (out of 10) of the challenge/appeal process. Incorrect Data Challenge (JDC), Uncorrected Data Adjustments (UDA), New Data Adjustment (NDA), and Loan Servicing Appeals (LSA). The system allows schools to submit these challenges and appeals during the cohort default rate appeal cycle. The system tracks the entire life cycle of each challenge/ appeal from the time it is submitted until the time a decision is made on it and it is closed. the eCDR Appeals system utilizes an oracle database provided on a Storage Area network (SAN).

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

The information contained in this system is maintained for the following purposes relating to students and borrowers:

1. To allow schools to electronically challenge their draft cohort default rate data via an incorrect data challenge, and electronically request an adjustment to their official cohort default rate data via an uncorrected data adjustment, new data adjustment or loan servicing appeal.

2. To allow Data Managers to electronically view and respond to cohort default rate challenges and adjustment requests from schools. Data Managers are determined on the basis of the holder of the loan. For FFEL loans held by the lender or its guaranty agency, the guaranty agency is the Data Manger for the purpose of the appeal. If the Department is the holder of the FFEL loan, then the Department is the Data manager. For direct loans, the loan servicer is the data manager.

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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

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? If this is an update, please include the publication date of the original.

Updated PIA Original Publication Date: 12/07/2007

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

Agency

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?

eCDR Appeals is considered a system of records under Privacy Act and maintains records under the following authority:

-OMB 1845-0022
-The Higher Education Act of 1965, As Amended, Section 441 and 461 Title IV, Section 401.

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? Please answer **YES** or **NO**.

Yes

2.2.1 ☐ N/A If the above answer is **YES** this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name and number, or indicate that a SORN is in progress.

Electronic Cohort Default Rate Appeals (eCDR Appeals). Federal Register number Vol. 80, No.182 September 21, 2015 p.569696

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 Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Schedule locator #078, NARA Disposition Authority Number: NI-441-08-11.
Records are temporary. Files are cut off annually after review of all official cohort default rate adjustments/ appeals for that cohort fiscal year. Records are destroyed 10 years after cut off.

[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

2.4 Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer **YES** or **NO**.

Yes

3. Characterization and Use of Information

Collection

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

The eCDR Appeals system contains records containing:

1. Student/borrower identifier information, Social Security Number, name, and date of birth.
2. Loan information (e.g. last date of attendance, date entered repayment, default date, etc.) for each student/ borrower loan counted in the cohort default rate of the school submitting the cohort default rate challenge or adjustment request; and
3. Documentation submitted by a school or data manager to support its data allegation(e.g student/ borrower SSN, name, enrollment verification, copies of canceled checks, etc.) the eCDR Appeals system does not collect any data directly from students/borrowers but stores PII data as it is received from schools.

3.2 Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer **YES** or **NO**.

Yes

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

School, guaranty agencies, loan servicers.

3.4 How is the information collected from stated sources (paper form, web page, database, etc.)?

Web page data entry and file upload.

3.5 How is this information validated or confirmed?[3]

Social Security Numbers are validated by format (i.e. 9-digit all numeric). Information entered on the web page or uploaded is verified by comparing that data against the internal data inside the ECDRA system.

[3] Examples include form filling, account verification, etc.

Use

3.6 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The Department will disclose borrower loan records to the postsecondary school or Data Manager responsible for the accuracy and completeness of the loan information, in order to obtain clarification or additional information to assist in determining the outcome of the school allegations. This use is directly consistent with the programmatic purpose of the system to:

1. Allow schools to electronically challenge their draft cohort default rate data via an incorrect data challenge, and electronically request an adjustment to their official cohort default rate data via an uncorrected data adjustment, new data adjustment, or loan servicing appeal.
2. Allow Data Managers to electronically view and respond to cohort default rate challenges and adjustment requests from schools. Data Managers are determined on the basis of the holder of the loan. For FFEL loans held by the lender or its guaranty agency, the guaranty agency is the Data Manager for the purpose of the appeal. IF the Department is the holder of the FFEL loan, then the Department is the Data manager. For Direct Loans, the Loan servicer is the Data Manager.
3. Allow Federal Student Aid to electronically view and respond to cohort default rate challenges and adjustment request from schools.

3.7 Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

No

3.7.1 ☒ N/A If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

3.8 Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 ☒ N/A If the above answer is **YES,** please explain.

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 system collect Social Security Numbers? Please answer **YES** or **NO**.

Yes

3.9.1 ☐ N/A If the above answer is **YES,** explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

The eCDRA system does not collect or ask for Social Security Numbers directly from users or borrowers; however, the system retrieves loan information from NSLDS that includes borrower SSN and stores and retains them in the application database. The system uses the SSN because it is the most reliable way to match information that may come from multiple sources to ensure that they are for a specific borrower. The different sources may, and usually do, use primary IDs that do not match each other and the SSN is the only constant identifier used in common. For example, a school may have a student ID for a student, and a loan servicer may have loan IDS for the student's loans, but the two IDs would be completely unrelated. The only way to match the records would be to use the SSN.

3.10 ☐ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

No alternatives were available at the time the eCDR Appeals system was created and no useful alternative has become available. The system uses the SSN because it is the most reliable way to match information.

The SSN is the unique identifier for the Title IV programs and its use is required by program participant and their trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under Federal law and regulations. Trading partners include the Department of Education, Internal Revenue Service, and institutions of higher education, nationwide consumer reporting agencies, lenders, and servicers.

4. Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The eCDRA System does not collect information or PII from users other than whats required to authenticate them as an authorized user and to monitor the site for any unauthorized access. Authorized users include school administrators, third party servicers, and FSA users. The eCDRA system does, however, retrieves loan information from NSLDS that includes borrower SSN and stores and retains them in the application database.

The user is presented with the Privacy Act Notice each and every time they log in to the application. They must review and accept the notice before being allowed to access the application.

4.2 ☐ N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

https://studentaid.ed.gov/sa/privacy

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Students and borrowers do not have the option in eCDR Appeals to consent or decline to provide information as they do not directly enter their information into the system. Their PII is included in the loan information that is entered into the system.

The eCDR Appeals system does not require personal information from the users (e.g. school, Data Manager, or FSA users) other than what's required to authenticate them in the system. Users are presented a Privacy Act notification page and a Rules of Behavior (the Rules) page after logging in where they may choose to cancel out before getting to the application pages.

5. Information Sharing

Internal

5.1 Will information be shared internally with other ED organizations? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.4.

Yes

5.2 ☐ N/A What information will be shared and with whom?

The information shared with other ED organizations will typically not contain any PII. Information on the results of the challenges, appeals, and adjustments, including final determination letter, may be shared on an ad-hoc basis, with the regional offices, Default Prevention, NSLDS, and other internal organizations.

5.3 ☐ N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The information on the results of the challenges, appeals and adjustments may be shared on an ad-hoc basis, with internal organizations who deal with default prevention assistance, management inquiries, etc. Final determination letter, generated by the system based on the result of adjustment requests, may be shared with the regional offices who uses the data for monitoring of the school's administrative capability.
These activities align, and are complementary to, the stated purpose in Question 1.2

External

5.4 Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer **YES** or **NO**. If the answer is **NO**, please skip to Question 5.8.

No

5.5 ☒ N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers, externally, please specify to whom and for what purpose.

5.6 ☒ N/A What is the purpose for sharing the specified information with the specified external organizations? Does this purpose align with the stated purpose in Question 1.2 above?

5.7 ☒ N/A How is the information shared and used by the external entity?

5.8 ☒ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer **YES** or **NO**.

No

5.9 ☐ N/A Does the project place limitation on re-disclosure? Please answer **YES** or **NO**.

Yes

6. Redress[4]

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

Procedures for allowing individuals to access their own information are outlined in the System of Records notice, which is location at: https://www.govinfo.gov/content/pkg/FR-2015-09-21/pdf/2015-23633.pdf

[4] If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.

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

Procedures for allowing individuals to correct their own information are outlined in the System of Records notice, which is location at: https://www.govinfo.gov/content/pkg/FR-2015-09-21/pdf/2015-23633.pdf

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

Procedures for telling individuals to correct their own information are outlined in the System of Records notice, which is location at: https://www.govinfo.gov/content/pkg/FR-2015-09-21/pdf/2015-23633.pdf

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? Please answer **YES** or **NO**.

Yes

7.2 What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

The eCDR Appeals application uses the Access and Identity Management System (AIMS) to authenticate users and verify that they are allowed to access the system. After authentication, the eCDR Appeals system uses a layered security implementation to control user access to information. The first layer encountered by users is the pages access layer. There are three basic types of users, school, data managers, and FSA users. This layer controls which pages specific user type have access to.

The next layer of security is a records level layer. At this level, users are limited to records where they have permissions. This layer uses a more detailed Access Control List (ACL) feature of the security framework than the page layer. An ACL is generated for each record identifying the organizations that should have access to records. The ACL can identify multiple organizations that have access to the records.

The third layer provides field level security. This uses a rules-based security framework that identifies specific fields that a user may have read or write access to.

Which users have access to the records and what level based on the business process workflow that were identified during the requirements phase of the project.

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

The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. Records are stored in a database on the Department's secure servers, and via other controlled electronic media. Records containing PII in the database are encrypted when at rest and are decrypted "on-the-fly" only when they are retrieved. Access to the eCDR Appeals system is limited to authorized personnel only. Authorized personnel retrieve records by school OPEID number and borrower Social Security number. They access records over the Internet over encrypted connections using secure protocol with government approved cipher suites. Individuals must review, and agree, to follow the eCDR Appeals system Rules of Behavior. These outline good security practices and stipulate consequences of a failure to comply.

FISMA controls implemented by eCDR comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, data minimization and retention (DM), data quality and integrity(DI), Transparency(TR), security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

7.4 Is an Authority to Operate (ATO) required? Please answer **YES** or **NO**.

Yes

7.5 Is the system able to provide account of any disclosures made? Please answer **YES** or **NO**.

No

7.6 Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

The Next Generation Data Center (NGDC) and the General System Support (GSS) provider, where the eCDR Appeals system is hosted, provide a comprehensive set of management, operational and technical security control in accordance with NIST Special Publication 800-53, Revision 4, "Security and Privacy Control for Federal Information System and Organization" and meet all the requirements of the Federal Information Security Management Act of 2002. These security controls include, but are not limited to, physical and environmental protection; personnel security; awareness and training; auditing and periodic risk assessments and security authorizations; policies and procedures; and technical controls such as firewalls, identification and authentication and other logical access controls, intrusion detection system, and regularly scheduled vulnerability scanning and security software updates. Access is restricted by eCDR Appeals system based on the user's role and assigned responsibilities within the organization.

8. Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

NIST SP 800-53 controls implemented by eCDRA comprise a combination of management, operational, and technical controls to ensure that information is used in accordance with approved practices.

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

Privacy risks of unauthorized disclosure of PII are mitigated by limiting access to eCDR Appeals system. All users of this system of records are given unique user identification and are required to establish a password that adheres to the Federal Student Aid Information Security and Privacy Policy (this policy requires a complex password that must be changed every 90 days). An automated audit trail documents user activity of each persona and device having access to eCDR Appeals system. The eCDR system has completed a formal security assessment and is now enrolled in Federal Student Aid's (FSA's) Ongoing Security Authorization (OSA) program. Under the OSA Program, the eCDR Appeals system NIST 800-53 controls are continually assessed on a quarterly basis per an OSA security control test schedule. The results of the OSA security control test are documented by FSA's security control assessment team. Transparent data encryption is used to protect data at rest, all websites and services provided by this system are available only through a secure connection(HTTPS) using DHS mandated protocols, weekly review of eCDRA application logs, secure remote VPN access for all privileged support users, web application firewall to protect, detect monitor, alert, or block attacks such as SQL injection and cross-site scripting, privileged account security/ logging/ auditing to reduce the risk of misused privileged insider attack.