NCUA
National Credit Union Administration

Privacy Impact Assessment for Enterprise Central Data Repository (ECDR)

Fiscal Year 2026

[This page intentionally left blank]

About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, to determine the privacy risks associated with an information system or activity, and to evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[1] Completion of a PIA is a precondition for the issuance of an authorization to operate.[2]

Basic Information about the System

System Name: Enterprise Central Data Repository Enterprise Central Data Repository (ECDR)

NCUA Office of Primary Interest: Office of the Chief Information Officer

Threshold	
Describe the system in 1-2 sentences.	The Enterprise Central Data Repository information system is an enterprise data repository and business intelligence solution that provides the central location for storing and managing NCUA's enterprise data for analytics and reporting, and which stores and maintains data in the original and processed forms for a secure and reliable enterprise storage system. The components of ECDR reside within the NCUA General Support System (GSS) on-premise environment. ECDR consists of enterprise data analytics software, database software, database servers, application servers, and the supporting infrastructure of the GSS. The users of the system are NCUA employees and uses of data from the

[1] 44 U.S.C. § 3501, note; Pub. L. 107–347, § 208(b).
[2] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).

	repository are used for a wide range of purposes such as reports related to NCUA events or NCUA financial information. Specifically, ECDR includes ONES loan analysis, Home Mortgage Disclosure Act Data Cube, ESS Data Sharing, Risk Assessment and Data Analytics Rating Dashboard (RADAR), SQL Server Data Marts, Informatica, and MicroStrategy components. ONES Loan Analysis provides Quality Control and Stratification reports for use by ONES financial analysts and lending specialists in monitoring and remediating data quality issues. It includes: Dashboards for use by the National Lending Specialists (and others) in the analysis and evaluation of Mortgage, Equity, Credit Card, Auto, Student and Other Consumer Loans; Reporting objects to enhance and facilitate ad-hoc reporting; and Reports to support analysis of historical data quality trends. For the Credit Union examiners, it provides the following functionality to assess loan-related risk for the nation's largest credit union: Structured and standardized loan data across multiple time periods in a single, secure repository; Access to loan data at any time, in advance of onsite examinations; Dashboards and reports that support risk-based "what if" analysis and forecasting; Ad hoc reporting/analysis capability and data exploration. It also provides authorized privileged users access to specific dashboards and reports, in addition to system administrative accounts. The account IDs are tokenized, so the NCUA is unable to identify which account belongs to which credit union member. The Home Mortgage Disclosure Act (HMDA) provides a published cube of the data such that users that have appropriate access to the data can create and save their own reports and visualizations. The data contains all mortgage loans for all banking institutions

	that are required to disclose their data for analysis of their fair lending practices. The data is used by other NCUA lines of businesses to perform this analysis on the loans that are sourced from the credit unions. The ESS Data Sharing is a functionality. It provides Legacy application and ESS data that can eventually be used for reporting and analytics within ECDR. Functionality in future phases will include exposure of additional data within ECDR reporting facilities. RADAR dashboard displays risk metrics across credit risk, liquidity risk, operational risk, and stress testing. This enables field staff to review credit union operating areas to determine the ongoing supervisory needs for the credit union. SQL Server Data Marts are smaller groupings of data pulled from the ECDR repository environment. Offices receive role-based access to the data marts. The Data Marts are outlined in a separate PIA. Informatica and MicroStrategy are business intelligence tools that reside within the ECDR environment so certain data from the environment can go into the software. Informatica is a data integration and management tool that analyzes/processes large amounts of data. For example, OCIO temporarily imports liquidated CU information from AMAC into the ECDR environment (resides in the ECDR environment for about 20 minutes), and reports are created utilizing that data in Informatica. The data is then removed from the ECDR environment. For OCFO, data from Delphi (NCUA financial information-Delphi has a separate PIA) is brought into ECDR and Informatica is used to process the data.

	MicroStrategy is utilized by OCFO as a business innovation tool. NCUA financial data (not CU data) that those offices are approved to access are provided to those offices to then utilize MicroStrategy to create reports. MicroStrategy is also used for MERIT, but is a separate use with a team used license. In 2026, OCFO will no longer use MicroStrategy. MicroStrategy was used in ECDR, but now ECDR utilizes Data Marts and Power BI. Some MERIT Data is deposited in ECDR and utilized in the Data Marts such as masked account information, CAMELS form fields, exam form report extracts, risk assessment extracts, and SSA account information (only the account name and group the SSA belongs to).

Artificial Intelligence		
1	*Are there Artificial Intelligence (AI) capabilities utilized in this system/service?* *AI is defined as a machine-based system that can, for a given set of human-defined objective, make predictions, recommendations or decisions influencing real or virtual environments.*	No

Purpose and Authority

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.

The NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained

in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Purpose and Authority		
1	*What is the purpose of the system?*	• NCUA information technology support. • General mission support.
2	*Why is the PII necessary to achieve the purpose described above? Also please indicate if only used for login/account creation purposes.*	The NCUA employees' and contractors' PII is collected to manage and maintain user accounts. The NCUA Credit Union examiners' name, work email, phone number and Employee ID # are maintained to identify who may have conducted the examination in order to verify the accuracy of the information in the system. The PII is collected when an examiner initially creates a CU examination report. A CU's CEO's phone number and address from CU Online is also located in ECDR as it provides analytical value for the agency. AMAC liquidation information is included to identify the individual, but their information is then deleted once it is digested in Informatica. Credit score/history and loan/share information is used by ONEs for analysis, but the account that it belongs to is tokenized so a particular individual. NCUA financial information located in Delphi is synthesized for OCFO through Informatica.
3	*What is the legal authority to collect, maintain, use, or share the PII contained in the system?*	12 U.S.C. § 1751 et seq.

Minimization

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.

The NCUA recognizes the increased sensitivity of Social Security numbers (SSNs) and therefore makes every effort to limit the collection and maintenance of them. The NCUA also limits its collection of other types of PII to those that are necessary.

SSNs		
1	*Will the system collect, maintain, or share social security numbers?*	Yes
1a	*How are SSNs displayed?*	AMAC Data in Informatica: The SSNs from AMAC liquidations are temporarily input into ECDR. They are transferred into Informatica, the output is created, and the SSNs are deleted (in ECDR for approx. 20 min).
1.1	*Of whom?*	• CU Members
1.2	*What is the law that authorizes this collection of SSNs?*	12 U.S.C. § 1751 et seq.; NCUA Rules and Regulations Part 741.
1.3	*Why are SSNs needed (i.e. how will they be used in the system)?*	The SSNs are temporarily used to identify the account holder and then deleted once the output is created.
1.4	*Why would using a less sensitive identifier or group of identifiers be insufficient*	The use of the SSN in the ECDR environment is temporary and is pulled from another system into ECDR in order to identify the account holder.
1.5	*Approximately how many unique SSNs will be maintained in the system?*	More than 100,000

PII		
1	*Basic Demographic*	• Email Address • First Name • Home Address • Last Name • Middle Name (or initial) • Phone Number
1.1	*Whose PII is collected?*	• CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: SSAs

2	*Medical and Family*	• None
3	*Financial*	• Account Number • Credit Score / Credit History • Loan and Share Information • Other: Informatica uses AMAC liquidation information such as SSNs, account number, and account balances, but it is only temporarily stored in ECDR (about 20 minutes). MERIT loan task data includes name, address, and account number, but the account number will be masked so the full account number is not sitting in ECDR, but can later identify the individual if there are fraud patterns found when utilizing the data output.
3.1	*Whose PII is collected?*	• CU Members • CU Officers, Employees, Volunteers
4	*Biometric*	• None
5	*Employment and Education*	• Other: Industry and organization name is collected for NCUA event enrollment.
5.1	*Whose PII is collected?*	• CU Members • CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: Public that signs up for NCUA events.
6	*Information Technology (IT)*	• Username • Unique Device Identifier • Tracking Data (Cookies, Web Beacons, geolocator, website engagement, IP Address, etc.)
6.1	*Whose PII is collected?*	• NCUA Contractors • NCUA Employees
7	*NCUA Employment*	• NCUA Email Address • NCUA Employee ID Number • NCUA iPhone Number • NCUA Office Phone Number
7.1	*Whose PII is collected?*	• NCUA Contractors • NCUA Employees

Collection and Consent

The NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

The NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. The NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

The NCUA endeavors both to collect information from the subject individual, and to attain affirmative informed consent, whenever possible. The NCUA's use of Privacy Act statements and privacy notices on forms are critical to this effort. For more information see the Transparency section below.

Collection and Consent		
1	*What are the sources from which the PII will be collected?*	• Existing NCUA information system
2	*Will the individuals whose information is collected/maintained in the system consent to their personal information being collected/maintained?*	Not specifically, but the individuals voluntarily chose to provide the information to NCUA.
3	*Will individuals be able to "opt-out" by declining to provide PII or by consenting only to a particular use?*	No
3.1	*Please explain.*	ECDR is the repository and includes business innovation solutions for the data, ECDR does not collect new data. The "opt out" to provide PII option is determined by the PII collected at the individual system level.

Procedures to Address Individuals' Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to complaints, concerns, and questions from individuals about the NCUA's privacy practices. The process is described on the NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Maintenance, Use, Sharing and Security

The NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

The NCUA implements, documents, and tests security and privacy controls as required by applicable NIST and OMB guidance. Access controls are of particular importance with regard to protecting individuals' privacy. Records management, both keeping records for the required time frame and timely destroying or accessioning them, is also a key component of managing privacy risks.

Maintenance and Use		
1	*Which statement is most accurate?*	NCUA owns the System.
2	*Describe how the role-based access is implemented to safeguard PII in this system/service.*	All NCUA staff have access to ECDR, but access is limited to the specific role membership and data is provided based on requests from offices.
2.1	*Based on what was described above, approximately how many individuals have elevated or administrator access to PII? Elevated access includes access that allows individuals to see PII other than their own individual PII.*	There are 4 developers that have administrative access to the entire environment.

Sharing and Security		
1	*With whom will the information be shared?*	• Within NCUA
2	*This system will require the following security review:*	ATO - Authorization to Operate

Records Management		
1	*Which records retention schedule(s) will apply to this system?*	• NCUA Record Schedule - Program Records • General Record Schedule - Finance (GRS 1.0) • General Record Schedule - Technology (GRS 3.0) • General Record Schedule - Mission Support (GRS 6.0)
2	*Please specify the records schedule (i.e. GRS 1.1, etc. or N1-413-0X-X Series X, Item X).*	GRS 1.1, 1.2, 1.3; GRS 3.1 and 3.2; GRS 6.3, Item 020 (DAA-GRS-2017-0009-0002); N1-413-02-2, Series 1, Items a, b1, b2, c, and d; N1-413-02-2, Series 2, Items a, b, c, and d; N1-413-02-2, Series 4, Items a, b, c, and d; N1-413-02-2, Series 10, Items a, b, c, and d, and DAA-0413-2022-0002.

Controlled Unclassified Information		
1	*Does the system/service contain records with CUI?*	Yes
1.1	*Are CUI markings utilized in the system/service?*	Yes
1.1a	*Select all that apply:*	• In-system
1.2	*Has this system/service been reviewed for security measures that meet CUI safeguarding requirements under 32 CFR § 2002.14, such as an ATO or ATU?*	Yes

Transparency

The NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

The NCUA's transparency efforts include providing adequate notice to individuals prior to collection of their PII. The NCUA achieves this with Privacy Act statements, or privacy notices (the latter if the collection is not associated with a Privacy Act System of Records), and compliance with the Paperwork Reduction Act.[3] The NCUA also publishes Systems of Records Notices in the Federal Register and makes them available on the privacy page of the NCUA's website.

Transparency		
1	*Will any forms or surveys be used to collect the information?*	No

SORNs		
1	*Is the information in the system retrieved by a personal identifier?*	Yes
2	*Applicable SORN*	NCUA-22

Accountability

The NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. The NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on the privacy page of NCUA's website), the NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Acceptable Use Policy and applicable Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must

[3] See the Collection and Consent section above.

protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of applicable Rules of Behavior upon gaining access to the NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[4]

Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

Analysis and Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy. Below are additional details regarding the review and approval of the PIA.

Analysis and Approval	
Privacy Risk:	Acceptable
Approval Date:	October 24, 2025

[4] 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.

facebook.com/NCUAgov

twitter.com/TheNCUA

linkedin.com/company/ncua

youtube.com/@NCUAchannel

1775 Duke Street | Alexandria, VA | 22314
703-518-6570
ncua.gov