NCUA
National Credit Union Administration

Privacy Impact Assessment for NCUA Connect

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: NCUA Connect NCUA Connect

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

Threshold	
Describe the system in 1-2 sentences.	NCUA Connect is comprised of the Okta FedRAMP Moderate authorized IDaaS. NCUA Connect provides identity management, authentication (including multi-factor authentication), course-grain authorizations, and a central user interface for all ESM program applications. Specifically, this system is the interface through which authorized users such as State Supervisory Authorities, Credit Unions, and Examiners access NCUA's examination, supervision, and reporting related systems. It provides a one-stop entry point for internal and external users.

[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).

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?*	• Credit union examination, supervision, enforcement action or liquidation. • 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 PII is necessary in order to provide users a multi-factor authentication to login into the NCUA Connect environment that hosts applications like MERIT.
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?*	No

PII		
1	*Basic Demographic*	• Email Address • First Name • Last Name • Middle Name (or initial) • Other: Individual's role and application access.
1.1	*Whose PII is collected?*	• CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: State Supervisory Authority staff (SSAs).
2	*Medical and Family*	None
3	*Financial*	None
4	*Biometric*	None
5	*Employment and Education*	None
6	*Information Technology (IT)*	• Username • Password • Answers to Security Questions • Login/Activity Records • Unique Device Identifier
6.1	*Whose PII is collected?*	• CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees

		• Others: State Supervisory Authority staff (SSAs).
7	*NCUA Employment*	• NCUA Email Address
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?*	• Directly from the individual the information is about • A Credit Union • Existing NCUA information system • Other: SSAs
2	*Will the individuals whose information is collected/maintained in the system consent to their personal information being collected/maintained?*	Yes, the individuals affirmatively consent to providing the information for the purpose and uses described in this system.
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.*	Users must provide basic information in order to gain access to the system.

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.*	NCUA's Tier 1 (OneStop) will have access to the PII from the Active Directory and then access authentication will be provided to the user with approval from OBI staff. The Tier 1 team can provide access to the different applications within the NCUA Connect environment. OBI staff can see the user's account information but cannot provision an account. For the applications in NCUA Connect, NCUA users' role is determined by their position at the agency-for example, an Eastern Region examiner can only see Eastern Region information.

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.*	Tier 1 OneStop employees.

Sharing and Security		
1	*With whom will the information be shared?*	• Within NCUA • Other Federal Agencies • Contractors • Other Third Parties: Individuals who are authorized users will only be able to access their own PII. SSAs and CU officers and supervisors will only be able to access the PII pertaining to their specific state or CU.
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?*	• General Record Schedule - General Operations Support (GRS 5.0)
2	*Please specify the records schedule (i.e. GRS 1.1, etc. or N1-413-0X-X Series X, Item X).*	GRS 3.2, Item 030 (DAA-GRS-2013-0006-0003)

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:*	• External Email Banner • Other: There are CUI banners in MERIT and MERIT is hosted within NCUA Connect.

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-21

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

[3] See the Collection and Consent section above.

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 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

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

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:	May 11, 2026

facebook.com/NCUAgov
twitter.com/TheNCUA
linkedin.com/company/ncua
youtube.com/@NCUAchannel

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