NCUA
National Credit Union Administration

Privacy Impact Assessment for CAPRIS

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: Consumer Access Process and Reporting Information System CAPRIS

NCUA Office of Primary Interest: Credit Union Resources and Expansion

Threshold	
Describe the system in 1-2 sentences.	The Consumer Access Processing and Reporting Information System (CAPRIS) provides a document management portal for NCUA's Consumer Access staff. There are two types of requests received in CAPRIS, the Phase I form and the Field of Membership expansion requests. Phase I form: The Phase I form is a form in which individuals desiring to charter a credit union can include preliminary information about the proposed credit union. Individuals filling out the Phase I form access CAPRIS through Login.gov. The Field of Membership (FOM) expansion requests: The Field of Membership expansion requests are requests from credit union officials to expand who is

[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).

	eligible to join a credit union. The credit union officials must submit their Field of Membership requests and the accompanying documents in CAPRIS. Credit Union officials access CAPRIS through NCUA Connect.

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?*	• 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 relevant and necessary for login purposes and for tracking, processing, and responding to requests submitted in the system.

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.; 12 U.S.C. § 1759 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*	• Birthdate, Age • Drivers License Number or State ID Number • Email Address • Fax Number • First Name • Home Address • Last Name • Middle Name (or initial) • Passport Number • Phone Number
1.1	*Whose PII is collected?*	• CU Officers, Employees, Volunteers • Others: Phase I form: In order to access and submit the Phase I form, individuals need to create a Login.gov account and a form of identification is required: U.S. Passport/Drivers License Number/ State ID Number. Their PII is also needed for the form.

		Field of Membership: PII is needed for login through NCUA Connect (Okta) and for the Field of Membership expansion request.
2	*Medical and Family*	None
3	*Financial*	None
4	*Biometric*	None
5	*Employment and Education*	None
6	*Information Technology (IT)*	• Username • Password • Login/Activity Records
6.1	*Whose PII is collected?*	• CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: Phase I form: Login.gov information. Field of Membership: Credit union officials' login through NCUA Connect. NCUA employees: Login information to access the Phase I form and Field of Membership requests. NCUA contractors: Login to troubleshoot any IT issues.
7	*NCUA Employment*	None

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
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.*	Phase I Form: In order for individuals to request to charter a credit union, they must provide their PII to use Login.gov in order to submit their Phase I form to NCUA and they must include their PII so NCUA can review their request to charter a credit union. Field of Membership: In order for credit unions to expand their field of membership and submit accompanying documents, they need to provide their login information to access CAPRIS through the identity and management solution (Okta) and provide the PII necessary to expand their field of membership.

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.*	Role-based access is limited to NCUA CURE staff reviewing and processing the requests. OCIO has administrator access.
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.*	NCUA's Tier 3 Helpdesk employees.

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 - 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).*	DAA-GRS-2022-0009-0002; N1-413-09-1, Series 1, Items A and F

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 • 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.

[3] See the Collection and Consent section above.

Transparency			
1	*Will any forms or surveys be used to collect the information?*	Yes	
	Title	***OMB No.***	***Privacy Act Statement or Privacy Notice?***
	Field of Membership Application	3133-0015	Privacy Notice
	Phase I Form	3133-0202	Privacy Notice

SORNs		
1	*Is the information in the system retrieved by a personal identifier?*	No

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 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:	February 25, 2026

[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