



Privacy Impact Assessment for NPW-NG

Fiscal Year 2025

[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 Public Websites – Next Generation NPW- NG

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

Threshold	
<i>Describe the system in 1-2 sentences.</i>	The NCUA Public Website- Next Generation's (NPW-NG) information system consists of interrelated components to implement NCUA.gov and MyCreditUnion.gov using the Drupal CMS framework and hosted on the Amazon Web Services (AWS) cloud platform.

Artificial Intelligence	
1	<i>Are there Artificial Intelligence (AI) capabilities utilized in this system/service?</i> <i>AI is defined as a machine-based system that can, for</i>

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).

	<i>a given set of human-defined objective, make predictions, recommendations or decisions influencing real or virtual environments.</i>	
1.1	<i>Describe the scope in which AI will be utilized. Please include any risks and impacts that utilizing AI will have on the system/service.</i>	AI is used for three different purposes on the NCUA websites: language translation, continuous monitoring for hacker/bot behavior, and searches. AI is used for language translation on the website. OMB and GSA require that the AI translation is proofread by a human linguist before it is published on NCUA.gov and MyCreditUnion.gov. AI creates a draft translation, then sends a notice to NCUA's contracted linguist, and the contracted linguist makes any corrections and marks for posting. Contract attached below. There is also AI continuous monitoring software that searches logs for hacker or bot behavior. Semantic search is AI consisting of machine learning (ML), natural language processing (NLP), and transformer models to understand what the user is searching for and matching their search language to the content they are searching. It applies contextual meaning rather than just matching keywords.

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.gov, social media platforms, public interface or other external communication management. • 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 PII collected/maintained/used in the system is necessary to more effectively communicate with individuals or groups and resolve issues with the NCUA stakeholders.
3	What is the legal authority to collect, maintain, use, or share the PII contained in the system?	12 U.S.C. § 1766, 1786, 1787, and 1789; 28 U.S.C. 2671-2680.

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) • Phone Number • Other: Home address is collected on the Speaker and Chairman's form.

1.1	<i>Whose PII is collected?</i>	• CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: Members of the public or other federal agencies.
2	<i>Medical and Family</i>	None
3	<i>Financial</i>	None
4	<i>Biometric</i>	None
5	<i>Employment and Education</i>	• Current Employment Information other than NCUA Employment (such as Occupation, Employer, Work Address, Work Phone, Work Email, Title, Salary) • Other: This PII and other related PII may be included in Letters of Prohibition and Administrative Orders (or other similar documents) that are published on the NCUA.gov.
5.1	<i>Whose PII is collected?</i>	• CU Officers, Employees, Volunteers • NCUA Employees • Others: Members of the public or other federal agencies.
6	<i>Information Technology (IT)</i>	• Username • Password • Login/Activity Records • Digital Certificate • Unique Device Identifier • Tracking Data (Cookies, Web Beacons, geolocator, website engagement, IP Address, etc.)
6.1	<i>Whose PII is collected?</i>	• CU Members • CU Officers, Employees, Volunteers • NCUA Employees • Others: Members of the public or other federal agencies.
7	<i>NCUA Employment</i>	• NCUA Email Address • NCUA iPhone Number • NCUA Office Phone Number
7.1	<i>Whose PII is collected?</i>	• 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 Federal Information System(s) • Another individual • Other: Since NCUA.gov is a public website, any person could submit information. The Speaker Request form may include the name and phone of secondary POCs identified by the submitter. All webforms have open-ended questions which could conceivably include PII if the submitter volunteers it.
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	No

	<i>consenting only to a particular use?</i>	
3.1	<i>Please explain.</i>	The individual voluntarily submits the form, so the individual is required to provide the minimal PII needed--first and last name and email address, in order to fulfill the purpose of the form.

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	<i>Which statement is most accurate?</i>	NCUA owns the System.
2	<i>Describe how the role-based access is implemented to safeguard PII in this system/service.</i>	There is role-based access and division of responsibilities so not all employees and contractors can view all of the information. The main roles are: view access, administrator access, and content management access.

2.1	<i>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.</i>	Approx. 10 people have oversight over all of the NCUA.gov information. Approx. 3 people have break-glass access. Approx. 11 people have access to all of the mycreditunion.gov information.
------------	--	---

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

Records Management		
1	<i>Which records retention schedule(s) will apply to this system?</i>	• NCUA Record Schedule - Program Records • General Record Schedule - Technology (GRS 3.0) • General Record Schedule - Mission Support (GRS 6.0)
2	<i>Please specify the records schedule (i.e. GRS 1.1, etc. or N1-413-0X-X Series X, Item X).</i>	DAA-GRS-2016-0013-0002; DAA-GRS-2013-0005-0005; DAA-GRS-2013-0005-0004; DAA-GRS-2013-0005-0010; DAA-GRS-2013-0005-0003; DAA-GRS-2017-0009-0002; and DAA-0413-2023-0006.

Controlled Unclassified Information		
1	<i>Does the system/service contain records with CUI?</i>	Yes
1.1	<i>Are CUI markings utilized in the system/service?</i>	Yes
1.1a	<i>Select all that apply:</i>	• External Email Banner
1.2	<i>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?</i>	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	<i>Will any forms or surveys be used to collect the information?</i>	Yes	
	Title	OMB No.	Privacy Act Statement or Privacy Notice?
	Speaker Request Form-Staff	3133-0211	Privacy Notice
	Website Feedback Form	N/A	Privacy Notice
	Speaker Request Form-Board	3133-0211	Privacy Notice

SORNs		
1	<i>Is the information in the system retrieved by a personal identifier?</i>	Yes
2	<i>Applicable SORN</i>	NCUA-23

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 staff electronically certify acceptance of their privacy responsibilities as a part of annual

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

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	
<i>Privacy Risk:</i>	Acceptable
<i>Approval Date:</i>	June 10, 2025



facebook.com/NCUAgov



twitter.com/TheNCUA



linkedin.com/company/ncua



youtube.com/@NCUAchannel

1775 Duke Street | Alexandria, VA | 22314

703-518-6570

ncua.gov