



Privacy Impact Assessment for NCUA GSS

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: General Support System NCUA GSS

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

Threshold	
<i>Describe the system in 1-2 sentences.</i>	The NCUA General Support System (GSS) provides the computing platform for all significant business applications for NCUA. The platform encompasses hardware, software, communications, network storage, databases, operating systems, and other infrastructure components. It also incorporates security measures, quality assurance processes, feedback mechanisms, management support systems, and safe workplace and productivity applications.

Artificial Intelligence		
1	<i>Are there Artificial Intelligence (AI) capabilities</i>	Yes

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>utilized in this system/service?</i> <i>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.</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>	Currently, the NCUA is undergoing an exploratory pilot of Microsoft Copilot, an AI tool. Risks and impacts are discussed in Privacy Impact Assessment (PIA) 378786.

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	<i>What is the purpose of the system?</i>	NCUA information technology support.
2	<i>Why is the PII necessary to achieve the purpose described above? Also please indicate if only used for login/account creation purposes.</i>	NCUA OPI's use OPI-owned applications that reside on the GSS computing platform to collect, create, maintain, and/or distribute the PII of NCUA employees, state examiners, credit unions, and contractors.
3	<i>What is the legal authority to collect, maintain, use, or</i>	The legal authorities to operate the NCUA GSS are:

	<i>share the PII contained in the system?</i>	5 U.S.C. 301, et seq. (Departmental Regulations); 12 U.S.C. Chapter 14 (The Federal Credit Union Act); and 40 U.S.C. Chapter 113 (Responsibilities for Federal information systems standards). The authorities that permit specific systems on the GSS to collect, use, maintain, and share PII are addressed in specific PIAs and SORNs.
--	---	---

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	<i>Will the system collect, maintain, or share social security numbers?</i>	Yes
1a	<i>How are SSNs displayed?</i>	NCUA OPIs use OPI-owned applications that reside on the NCUA GSS. The NCUA OPI application PIAs describe how SSNs are displayed in the underlying application.
1.1	<i>Of whom?</i>	• CU Members • CU Officers, Employees, Volunteers • NCUA Contractors • NCUA Employees • Others: SSAs
1.2	<i>What is the law that authorizes this collection of SSNs?</i>	The legal authorities to operate the NCUA GSS are: 5 U.S.C. 301, et seq. (Departmental Regulations); 12 U.S.C. Chapter 14 (The Federal Credit Union Act); and 40 U.S.C. Chapter 113 (Responsibilities for Federal information systems standards). The authorities that permit specific systems on the GSS to collect, use, maintain, and share SSNs are

		addressed in specific PIAs and System of Records Notices (SORNs).
1.3	<i>Why are SSNs needed (i.e. how will they be used in the system)?</i>	NCUA OPIs use OPI-owned applications that reside on the GSS computing platform to collect, create, maintain, and/or distribute the PII of NCUA employees, state examiners, credit unions, and contractors. The platform includes all major IT hardware, software, communications, network storage, central databases, operating systems, and other minor, infrastructure, security-related, and productivity applications. The NCUA GSS relies on the OPI application data owners to complete PIAs to document the information collection reason, as required.
1.4	<i>Why would using a less sensitive identifier or group of identifiers be insufficient?</i>	NCUA OPIs use OPI-owned applications that reside on the NCUA GSS. The NCUA OPI application PIAs describe the intended agency use for PII that is collected, created, maintained, and/or distributed.
1.5	<i>Approximately how many unique SSNs will be maintained in the system?</i>	More than 10,000

PII		
1	<i>Basic Demographic</i>	• Birthdate, Age • Drivers License Number or State ID Number • Email Address • First Name • Home Address • Last Name • Middle Name (or initial) • Phone Number • Race or Ethnicity • Sex
1.1	<i>Whose PII is collected?</i>	• CU Members • NCUA Contractors • NCUA Employees
2	<i>Medical and Family</i>	• Emergency Contact • Information about Spouse(s), Children, or other Family Members • Marital Status or Marriage/Divorce Records

		• Medical History • Reasonable Accommodation Information
2.1	<i>Whose PII is collected?</i>	• NCUA Contractors • NCUA Employees
3	<i>Financial</i>	• Account Number
3.1	<i>Whose PII is collected?</i>	• NCUA Contractors • NCUA Employees
4	<i>Biometric</i>	• Photograph • Signature • Voice Recording
4.1	<i>Whose PII is collected?</i>	• NCUA Contractors • NCUA Employees
5	<i>Employment and Education</i>	• Employment History
5.1	<i>Whose PII is collected?</i>	• NCUA Contractors • NCUA Employees
6	<i>Information Technology (IT)</i>	• Username • Password • Answers to Security Questions • 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>	• NCUA Contractors • NCUA Employees
7	<i>NCUA Employment</i>	• Drug Test Results • NCUA Email Address • NCUA Employee ID Number • NCUA Employment Performance Appraisal Information • NCUA iPhone Number • NCUA issued Credit Card Number and associated information • NCUA Office Phone Number • NCUA Training History
7.1	<i>Whose PII is collected?</i>	• 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	<i>What are the sources from which the PII will be collected?</i>	• Directly from the individual the information is about • Existing NCUA information system • Other: Data is collected for the purpose of creating the user account.
2	<i>Will the individuals whose information is collected/maintained in the system consent to their personal information being collected/maintained?</i>	Yes, the individuals affirmatively consent to providing the information for the purpose and uses described in this system.
3	<i>Will individuals be able to "opt-out" by declining to provide PII or by consenting only to a particular use?</i>	No
3.1	<i>Please explain.</i>	Use of the GSS is required for NCUA employment.

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>	Role-based access is done through Active Directory (AD); access to resources depends on the type of user account and permissions granted within AD. Specific roles are listed in the Authorization Package documentation.
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>	There are 42 individuals with elevated or administrator access to PII within GSS.

Sharing and Security		
1	<i>With whom will the information be shared?</i>	• Within NCUA • Other Federal Agencies • 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>	General Record Schedule - Technology (GRS 3.0)
2	<i>Please specify the records schedule (i.e. GRS 1.1, etc. or N1-413-0X-X Series X, Item X).</i>	The GSS computing platform is predominantly covered by the General Records Schedule 3.1, General Technology Management Records and General Records Schedule 3.2, Information Systems Security Records; GRS 3.1, item 020 (Information technology operations and maintenance records) is likely most relevant, but all items within those two schedules may be applicable. OPI-owned applications that reside on the GSS computing platform are covered by various records schedules that are listed in their respective PIAs.

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	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-27

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.

³ See the Collection and Consent section above.

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:	November 17, 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

11 ncua.gov