



Privacy Impact Assessment for Employee Pre-Hire and Subject Matter Expert (EPSME)

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: Employee Pre Hire and Subject Matter Expert Employee Pre-Hire and Subject Matter Expert (EPSME)

NCUA Office of Primary Interest: Office of Human Resources

Threshold	
<i>Describe the system in 1-2 sentences.</i>	The Office of Human Resources (OHR) at the National Credit Union Administration (NCUA) uses the Employee Pre Hire and Subject Matter Expert (EPSME) System as an intranet web application to enter, update, and view NCUA specific information when new hires are processed by HR Links to become employees. EPSME is comprised of two functional modules, Employee Pre-hire and Employee SME. The Employee Pre-Hire Module is the sole source for generating employee numbers for pre-hires (which is the official employee number going forward past the pre-hire process). The Employee SME Module allows authorized users to view historical employee subject

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).

	matter expert designation as well as provide SME reports for active or inactive employees. Once an NCUA employee onboards, EPSME is used to manage and maintain assignment changes. These changes are used to create system profiles for various NCUA systems (e.g. Merit, TMS, etc.).
--	--

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 a given set of human-defined objective, make predictions, recommendations or decisions influencing real or virtual environments.</i>	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	<i>What is the purpose of the system?</i>	Employee development, management, or benefit administration.
2	<i>Why is the PII necessary to achieve the purpose described above? Also</i>	Basic Demographic PII is necessary for EPSME to automatically generate employee numbers for each employee name in the system. NCUA Employment PII

	<i>please indicate if only used for login/account creation purposes.</i>	is necessary to create system profiles for employees that link to various NCUA systems (e.g., Merit, TMS, etc.).
3	<i>What is the legal authority to collect, maintain, use, or share the PII contained in the system?</i>	• Employees, 5 U.S.C. Part III • Numbering System for Federal Accounts Relating to Individual Persons, E.O. 9397 • Employees' account numbers, 26 CFR 31.6011(b)-2 • Supplying of identifying numbers, 26 CFR 31.6109-1

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>	No

PII		
1	<i>Basic Demographic</i>	• Email Address • First Name • Last Name • Middle Name (or initial)
1.1	<i>Whose PII is collected?</i>	• NCUA Employees
2	<i>Medical and Family</i>	None
3	<i>Financial</i>	None
4	<i>Biometric</i>	None
5	<i>Employment and Education</i>	None
6	<i>Information Technology (IT)</i>	None

7	<i>NCUA Employment</i>	• NCUA Email Address • NCUA Employee ID Number • 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	<i>What are the sources from which the PII will be collected?</i>	• Directly from the individual the information is about
2	<i>Will the individuals whose information is collected/maintained in the system consent to their personal information being collected/maintained?</i>	Not specifically, but the individuals consented to providing the information originally and likely anticipated that their information would also be maintained and used this way.
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>	The PII provided is to facilitate the employment of individuals seeking jobs at the agency. The identifying PII is required.

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>	OHR safeguards EPSME's PII by granting access to only a limited number of authorized users who have a need to know to perform their official duties. Access to EPSME is restricted to OHR, Office of National Examinations and Supervision (ONES), and Regional Division of Management Services (DMS) to enter potential new hire's basic demographic and organizational information. Role-based access in EPSME is as follows: • Admin Role - granted access to all actions in EPSME (i.e. Pre-hire and SME modules);

		- Pre-Hire Role - granted access for operations related to Pre-hire module (i.e. add, search, view, modify or withdraw pre-hire information); and - Employee - granted access for operations related to the Employee/SME module (i.e. view and run historical SME reports, and modify employment information, employee type, or district assignment).
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>	9 OHR and 6 Regional employees have administrator roles to view and change PII. 2 OCIO employees have access to view PII for backend operations and development purposes. 1 OBI employee has access for security review.

Sharing and Security		
1	<i>With whom will the information be shared?</i>	Within NCUA
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 - Human Resources (GRS 2.0)
2	<i>Please specify the records schedule (i.e. GRS 1.1, etc. or N1-413-0X-X Series X, Item X).</i>	GRS 2.2, Employee Management Records, Items 010 and 120

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	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 Act³ 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	OPM/GOVT-1

Accountability

The NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. The

³ See the Collection and Consent section above.

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

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	
<i>Privacy Risk:</i>	Acceptable
<i>Approval Date:</i>	October 15, 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