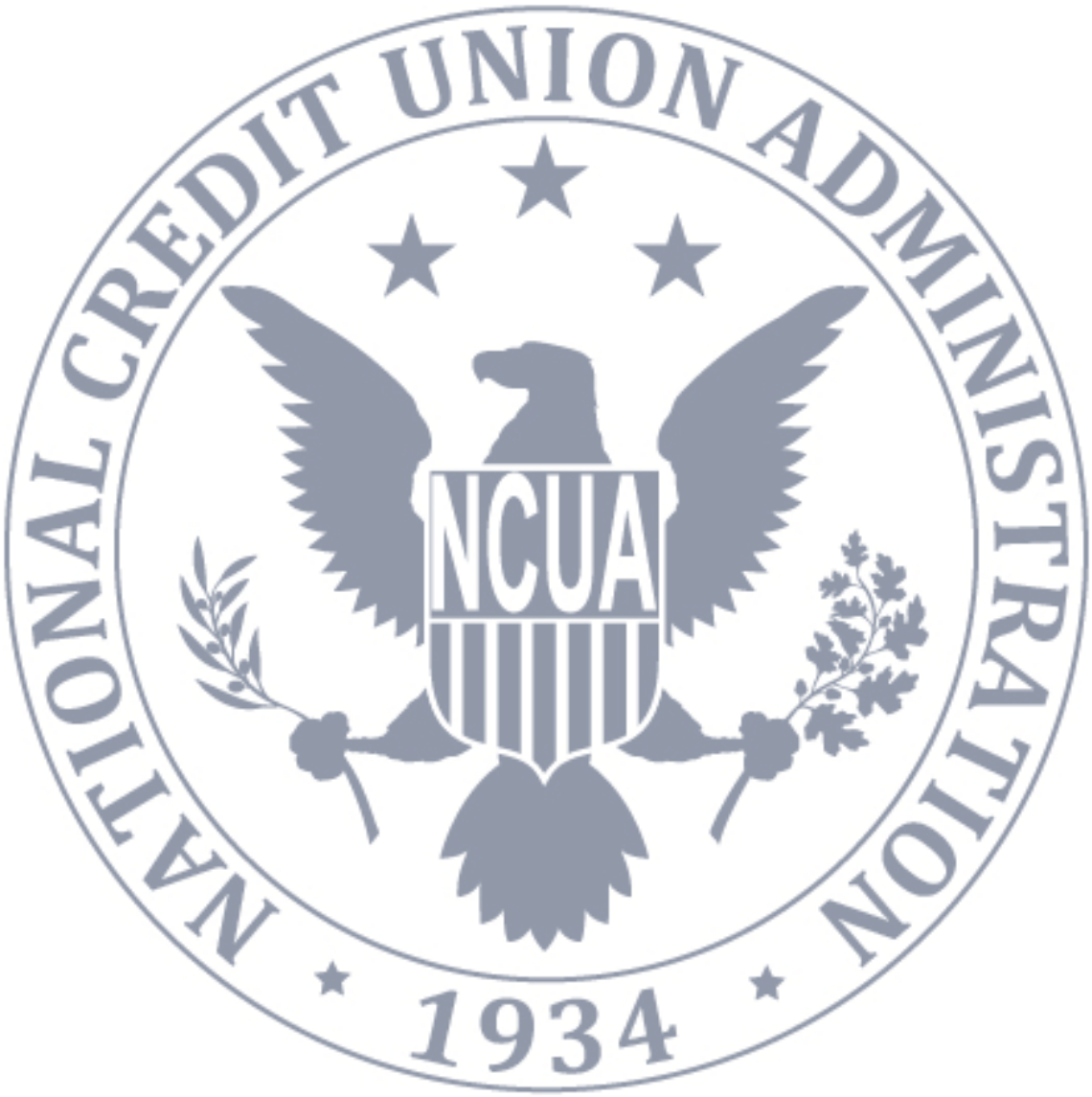
NCUA
National Credit Union Administration

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

Fiscal Year 2019

[This page intentionally left blank]



PIA for Employee Pre-hire and Subject Matter Expert (EPSME) • FY2019

Table of Contents

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, determine the privacy risks associated with an information system or activity, and 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]

A PIA form (and an automatic workflow and streamlined review and approval process) has been developed for consistency and ease of use. The form, and additional guidance about PIAs, is available for NCUA staff on the Privacy team's intranet site.

The Privacy team is responsible for reviewing and approving PIAs, preparing approved PIAs for publication, and otherwise managing the PIA process.

Basic Information about the System

System Name: Employee Pre-hire and Subject Matter Expert (EPSME)

NCUA Office Owner: OHR

System Manager: [redacted]

[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).

Authority

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.

Authority for the System

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

Purpose Specification and Use Limitation

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 of the System

EPSME is used by NCUA Office of Human Resources (OHR) and the Regional Division of Management Service Staff (DMS). PII information collected is used to generate a NCUA unique identifier and to mail equipment and any required communications to new hires. NCUA unique identifier and other non-PII information is extracted from EPSME and utilized by other NCUA internal applications.

Intended Use of the PII Collected

EPSME consists of three modules Pre-hire, Employee and SME. The Pre-hire module is used to generate a NCUA unique identifier for new hires as part of the onboarding process. Once the new hire becomes active, certain employment information (i.e. organization, employee type and district assignment, business email address) is collected and extracted from EPSME and utilized by other NCUA internal applications. SME module is used to capture and maintain Subject Matter Expert (SME) primary designations for principle examiners to assist with workload assignments in specialized areas.

Sharing of the PII

NCUA unique identifier and other non-PII information is extracted from EPSME and is used by other NCUA internal applications. Only NCUA Office of Human Resources (OHR) and Regional Division of Management Service Staff (DMS) have access to EPSME. EPSME does not have a mechanism to allow users to download and share PII data. Users only have the ability to download SME reports from EPSME which does not contain PII information. SME designations are shared with regional staff.

Minimization

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.

Types of PI Collected

EPSME is an intranet web application that collects the following PII information for NCUA new hire employees as part of the onboarding process and current employees as part of maintaining information for business related purposes.

1. First Name, Last Name, Middle Initial
2. Suffix
3. Home and Business Address (shipping and P.O. Box)
4. Telephone Number (work cell phone)
5. Email address (work)
6. Fax Number

Individual Participation

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. NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

Opportunity for Consent

Individuals consent to their personally identifiable information being stored in this 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 NCUA's privacy practices. The process is described on NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Quality and Integrity

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.

Source of the PII

Data is collected from OHR/DMS.

Security

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.

Safeguards

• The application is an intranet application, only users on NCUA network with approved access may have access to the data. Access is requested by the office, approved by OHR

and granted by OCIO.

• The application restricts access to information based on Users' specific authorization granted by NCUA Security Team. The process of collecting and modifying the pre-hire PII will be completed by NCUA employees from OHR and DMS staff that has been granted one or more of the following actions (Read, Create, Update, Withdraw, and SME Reports). These are grouped in two security groups: Admins (by default will have enabled all 6 actions) and Employee Pre-hire (that will have Create, Update and Withdraw actions). Being added to one or both of these groups will be achieved through the "NCUA Security Application" current process.

• The information is held in the system EPSME eternally, although pre-hire can no longer be viewed 60 days after the start date.

Transparency

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.

Applicable SORN

This system is covered by OPM/GOV-1.

Availability of Privacy Notices

The SORN and PIA for the Employee Pre-hire and Subject Matter Expert (EPSME) are publicly available on the privacy page of NCUA's website.

Accountability

NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. 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), 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 Computer Security 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 the Rules of Behavior upon gaining access to NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[3]

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.

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

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 4/10/19.