NCUA
National Credit Union Administration

Privacy Impact Assessment for NCUA LearnCenter

Fiscal Year 2018

[This page intentionally left blank]

PIA for NCUA LearnCenter • FY2018

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: NCUA LearnCenter

NCUA Office Owner: OHR

System Manager: [redacted]

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.*

[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 for the System

5 U.S.C., pt. III

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

We need the demographic information in order to:

- Create user accounts in the Learning Management System
- Assign training based on traits, such as supervisor status, occupational series, state examiner, etc.

Intended Use of the PII Collected

We need the demographic information in order to assign training based on traits, such as supervisor status, occupational series, state examiner, etc.

Sharing of the PII

PII in the system may be shared with:

- Supervisors and State Supervisory Authorities (SSA): They can see their employees' name/email, assignments and learning history);
- Instructors: They can see restricted user data in order to assign users to courses;
- LearnCenter Administrators (4 Federal and 2 contractors): They can see all user information; and
- Other individuals in the agency who have a specific need for access to specific information in the system (such as annual reporting requirements).

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 PII Collected

- Data collected for NCUA Employees and Contractors / State Examiners
- First Name X/ X
- Last Name X /X
- Day Phone X/ X
- Email X /X
- Email 2 /X
- Job Title X/
- Manager Name X/X
- EOD with NCUA X/
- Occupational Series Code X/
- Region/Office X/X
- SE Group/Division X/
- Duty Station City X/X
- Duty Station State X/X
- Date Arrived Present Position X/
- Supervisory Status X/
- Bargaining Unit Status X/
- Pay Plan X/
- Grade or Level X/
- Education Level Description X/
- Employee ID X/X
- Managed by Integration X/
- Supervisor ID X/
- OJT Name X/
- State Examiner? X/X
- Date Created X/ X
- Date Joined X /X
- Date Last Access X/ X
- Date Updated X/ X
- Status X/X

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

Due to the nature of this system, there is not an opportunity to ask individuals to consent.

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

NCUA Employees and contractor user data is provided by an OCIO Active Directory feed. State examiner user accounts are created by the State Training Coordinator.

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 system requires username and 8 character password with at least 1 capital letter, 1 lower case letter, and 1 number to access. Self-registration is not permitted. All users are added by the OHR LearnCenter administrators.

It is on a secured (https) Government cloud server and is categorized as FedRAMP "In-Process."

The PII on the system is only accessible to the OHR LearnCenter team and other individuals in the agency with a specific need.

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 NCUA-5; OPM/GOVT-1.

Availability of Privacy Notices

The SORN and PIA for the NCUA LearnCenter 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 12/18/17.