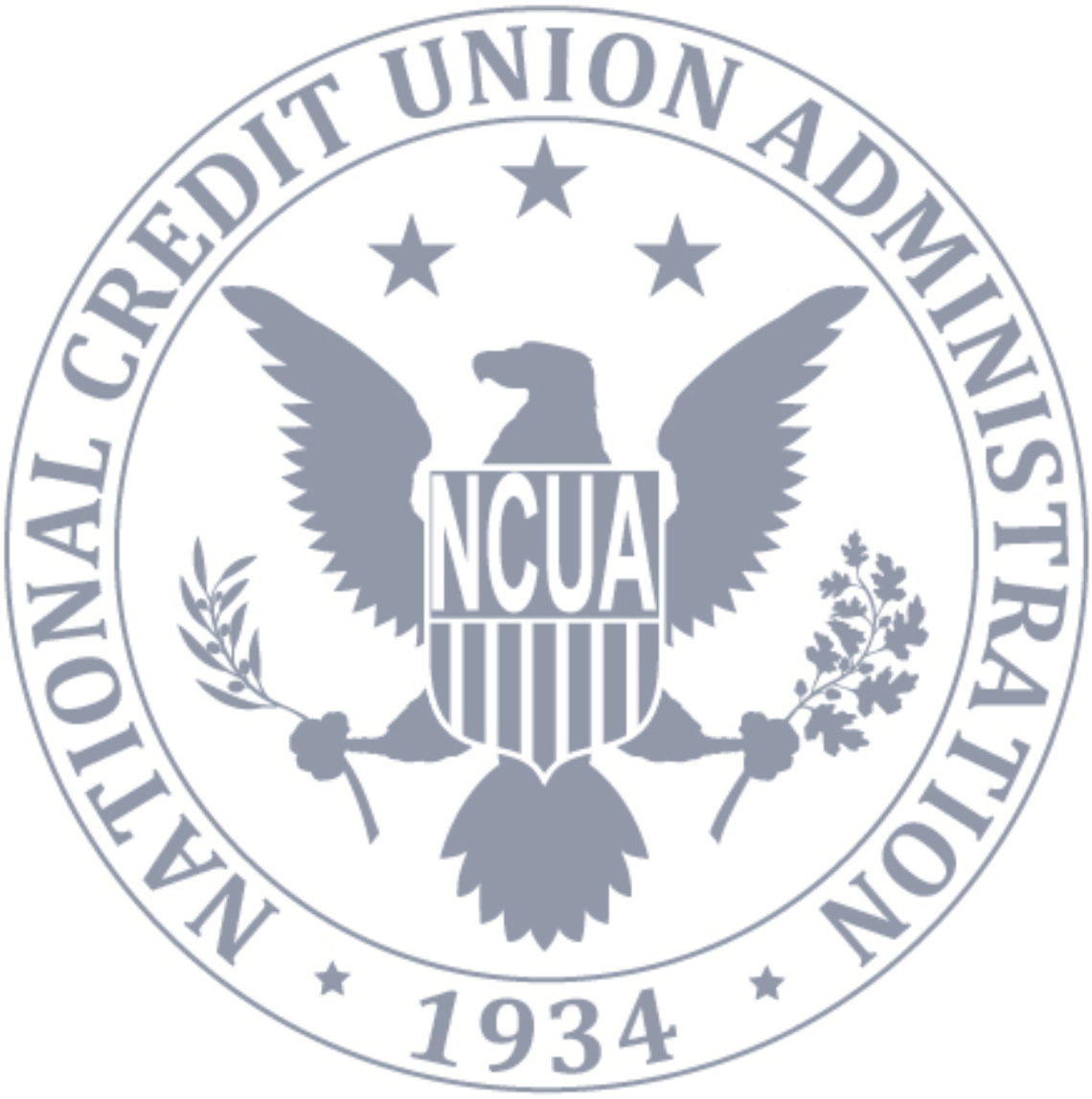
NCUA
National Credit Union Administration

Privacy Impact Assessment for CUSO Registry

Fiscal Year 2018

[This page intentionally left blank]



PIA for CUSO Registry • 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: CUSO Registry

NCUA Office Owner: Office of Examination and Insurance (E&I)

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

12 U.S.C. § 1751 et seq.

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

In order to implement the CUSO Registry as a web application, NCUA must create application user accounts for users to input the required CUSO registration information and update it annually, as required. Credit Union (CU) and State Supervisory Authority (SSA) users, who have a legitimate need for information housed in the system will also require user accounts. Security requirements for establishing online accounts include the identification and authentication of individual users, thereby creating the requirement for collection of PII (name and e-mail address).

NCUA requires contact information for the designated CUSO contact and Chief Executive Officer (CEO) (name and e-mail address) in order to contact the CUSO to fulfill NCUA responsibilities to oversee the safety and soundness of each credit union. The CUSO has the option of providing a company e-mail address for one or both of these individuals, but some CUSOs may use personal e-mail addresses, which constitutes PII.

A limited number of NCUA users will use CUSO owner information to determine which individuals have ownership interests in multiple CUSOs in order to determine ownership concentrations and interdependencies between CUSO's (owner name and city/state of residence) and any related supervised credit unions. Due to industry concentrations in the financial services sector, the failure of a single CUSO could impact one or more supervised credit unions.

Intended Use of the PII Collected

See Purpose above.

Sharing of the PII

The CUSO Registry system implements the concepts of "least privilege" and "separation of duties" by restricting access to data based on a user's profile. NCUA has implemented the concepts of "role based access" where each "role" defines the data an individual user may see and what actions a user may perform.

There are four general "roles" within the CUSO Registry system – NCUA users, credit union users, State Supervisory Authority users, and CUSO users. NCUA users, with approved access, will have access to the system information, including the PII. NCUA users will be granted access through Active Directory authentication only if the position requires access to the information in the performance of official duties. NCUA users primarily need the email information to contact CUSOs regarding their registration information and to maintain CUSO Registry user accounts.

Select credit Union (CU) CUSO Registry system users will have access to system information only for those CUSOs for which the registered CUSO has granted access. They require this information to contact the CUSO personnel and to review the information submitted by the CUSO.

The State Supervisory Authority (SSA) CUSO Registry system users will have access to CUSO data records. SSAs require this information to contact the CUSO personnel, review the information submitted by the CUSO for accuracy and completeness, and understand relationships between CUSOs and their owners.

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

The system collects individual names for CUSO contacts, CUSO Chief Executive Officers (CEOs), CUSO owners (those who are individual persons) and all individuals who establish CUSO Registry System online accounts. System users will be personnel designated by the CUSO, credit union personnel, and state supervisory authority personnel. NCUA personnel who require system access will use established NCUA accounts; the system will not collect additional PII about NCUA users. The system collects e-mail addresses for all the individuals listed, except the CUSO owners, for the

purposes of user account verification and management. For CUSO owners, the system collects the owner's name, city and state.

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 provide their personally identifiable information voluntarily.

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

CUSO users and all other non-NCUA users who establish CUSO system accounts will provide all information containing PII for the system. In most cases, the individual will provide his/her own PII, although the CUSOs may choose to have a CUSO representative (designated as the CUSO Admin) provide the information for the CUSO contact, CUSO CEO, CUSO owner(s), and other CUSO users. No PII will be obtained

from other systems.

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 privacy controls specified in NIST Special Publication 800-53r4, Appendix J Privacy Controls Catalog, will be implemented for the system based on the system security categorization and assessment of risk. These controls are specifically designed to protect the data from unauthorized access and misuse. Details on the implementation of these controls may be found in the CUSO Registry System Security Plan.

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-18.

Availability of Privacy Notices

The SORN and PIA for the CUSO Registry 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 7/13/17.