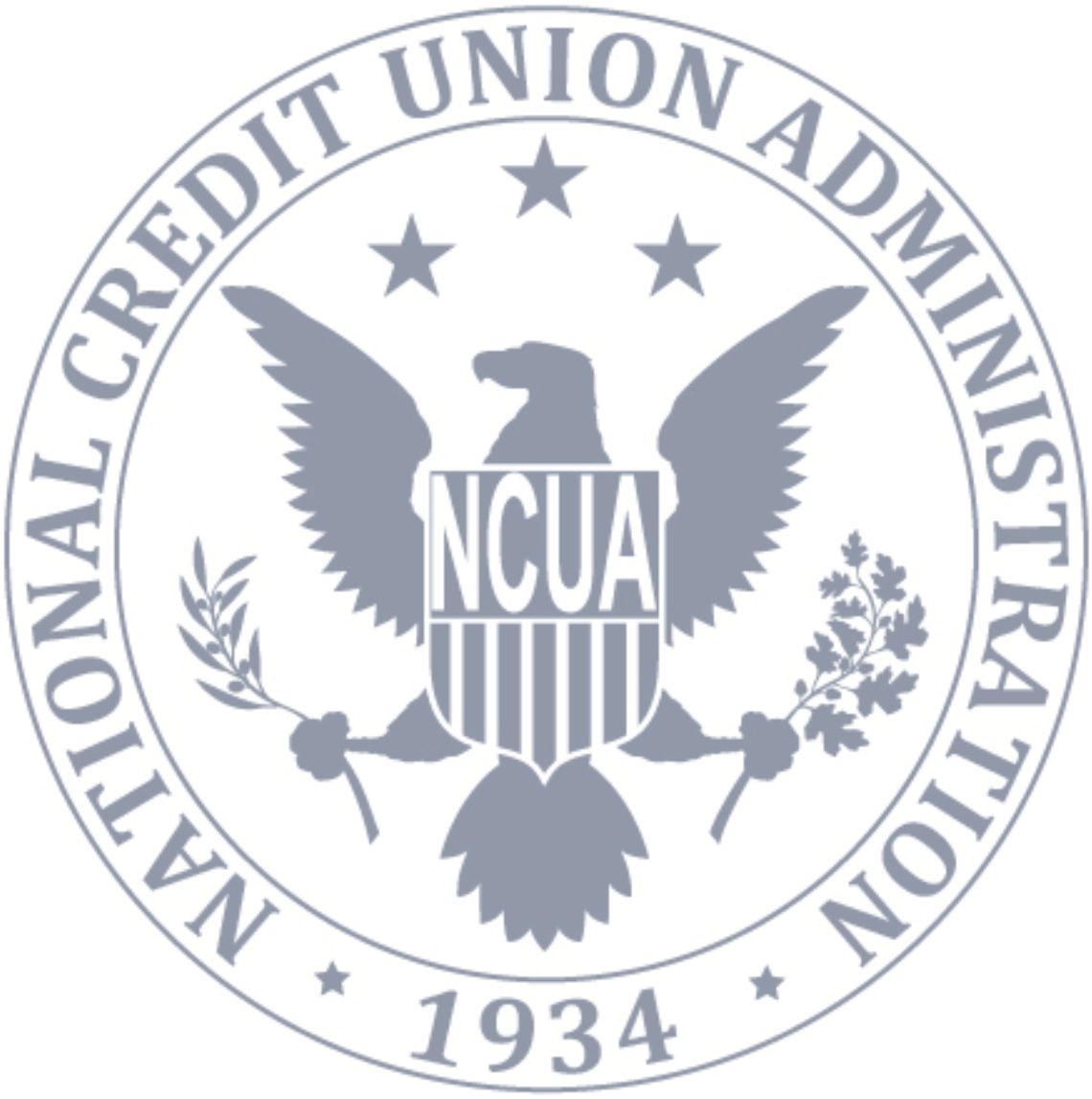
NCUA
National Credit Union Administration

Privacy Impact Assessment for CUOnline and Corp CUOnline

Fiscal Year 2018

[This page intentionally left blank]



PIA for CUOnline and Corp CUOnline • 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: CUOnline and Corp CUOnline

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

The purpose of collecting this information provides the ability to contact officials for various reasons (exam related discussions, mailing of an exam report, emergencies, etc.), monitoring and mitigating risk purposes (safety and soundness), and congressional reporting (this pertains to the minority deposit institution question).

Security requirements for establishing CUOnline and Corp CUOnline accounts include the identification and authentication of individual users, thereby creating the requirement for collection of PII (name and e-mail address).

Intended Use of the PII Collected

Intended agency use of the information includes the ability to contact officials for various reasons (exam related discussions, mailing of an exam report, emergencies, etc.), monitoring and mitigating risk purposes (safety and soundness), and congressional reporting (this pertains to the minority deposit institution question).

The PII remains in the system until the credit union or field staff update the collected information. CUOnline (including the Profile) is required to certified and validated on a quarterly basis (March, June, September, and December). Corp CUOnline is required to be certified and validated on a monthly basis. Credit unions must certify the information in the Profile for at least each cycle to ensure the information is current and accurate. In addition to the quarterly cycle certification, credit unions must update their Profile within 10 days after the election or appointment of senior management or volunteer officials, or within 30 days of any change to the information in the Profile.

Sharing of the PII

PII information is for internal NCUA purposes only and is not shared with the public.

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 PII is directly related to the NCUA Profile Form 4501A (CUOnline) and Non-Financial Form 5310 (Corp CUOnline). The Profile information is collected through CUOnline and Corp CUOnline. On the Contacts tab of the Profile, the system collects credit union individual information employed by or associated with the credit union. Specifically, Manager or CEO, Vice Chairperson, Board Treasurer, Supervisory Committee Chairperson, Credit Committee Chairperson, Chief Financial Officer, Internal Auditor, Board Chairperson, Board Secretary, Board Member, Supervisory Committee Member, Credit Committee Member, and Chief Information Officer. There is box to select other, which then requires them to fill in the name. In addition, the system identifies Patriot Act Contacts, Emergency Contacts, Information Security Contact, Profile Information Contact, and 5300 Call Report Contact. For all individuals listed, the system collects home address, home email, home phone number, home cell number, home fax, work address, work email, work phone number, work cell, work fax, and employment type.

On the Program and Services tab of the Profile for both CUOnline and Corp CUOnline, there is a minority depository institution question that could possibly lead to PII depending on the size of the board. The question asks if more than 50 percent of the credit union's current board of directors are Black American, Native American, Hispanic American, or Asian American. Specifically, in smaller credit unions with smaller board of directors, this question could potentially link race of individuals on the board.

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

CUOnline and Corp CUOnline Profile is where the data is collected from credit unions.

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 CUOnline System Security Plan. In addition, the privacy training is managed at the enterprise level.

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

Due to the nature of this system, a SORN is not required.

Availability of Privacy Notices

The PIA for CUOnline and Corp CUOnline 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 8/21/2017.