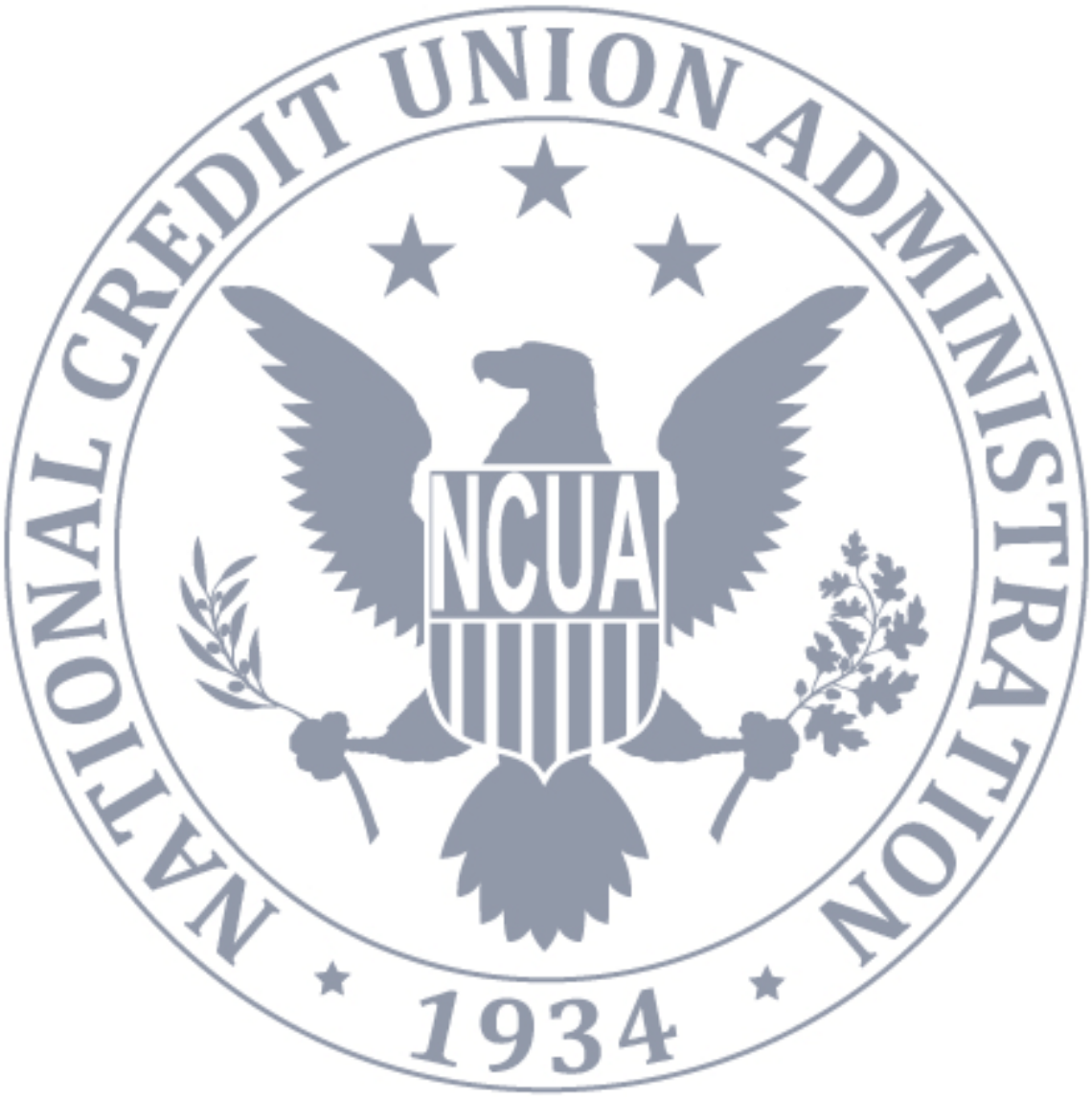
NCUA
National Credit Union Administration

Privacy Impact Assessment for NCUA FOIAXpress System

Fiscal Year 2018

[This page intentionally left blank]



PIA for NCUA FOIAXpress System • 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 FOIAXpress System

NCUA Office Owner: OGC

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. § 1789, 5 U.S.C. § 552, 5 U.S.C. § 552a

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 NCUA is obligated under federal law to comply with both the Freedom of Information Act and the Privacy Act. NCUA Office of General Counsel (OGC) has responsibility for processing Freedom of Information Act requests and appeals, as well as Privacy Act requests.

Intended Use of the PII Collected

The Office of General Counsel (OGC) uses FOIAXpress as an electronic document management system to manage the entire lifecycle of Freedom of Information Act (FOIA) and Privacy Act requests, and to store all FOIA-related records (requests, redacted and raw versions of responsive documents, responses, etc.). OGC also uses the system to produce statistical reports (for management purposes, as well as for the required Department of Justice Annual Report).

Sharing of the PII

No other systems share data with or have access to the data in the system.

Subject to the FOIA and Privacy Act, PII may be shared with internal staff and third parties. Seehttps://www.ncua.gov/services/Pages/freedom-of-information-act.aspx.

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 information collected is the agency Freedom of Information Act & Privacy Act requests & invoices, along with the records requested. The information may contain PII of NCUA employees as well as members of the public, such as credit union account holders, employees and others. The information may include personal and professional contact information, financial information, personal identifiers, and personal communications.

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

The data is collected from agency records and from members of the public.

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

FOIAXpress is FedRamp certified. Access is restricted via user accounts (user-id and password). Only individuals with FOIA job responsibilities are issued user accounts; currently, 4 individuals have accounts. User accounts are deactivated when an individual leaves NCUA or no longer has job duties that require access to the system.

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-9.

Availability of Privacy Notices

The SORN and PIA for the NCUA FOIAXpress System 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]

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

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.

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 5/4/17.