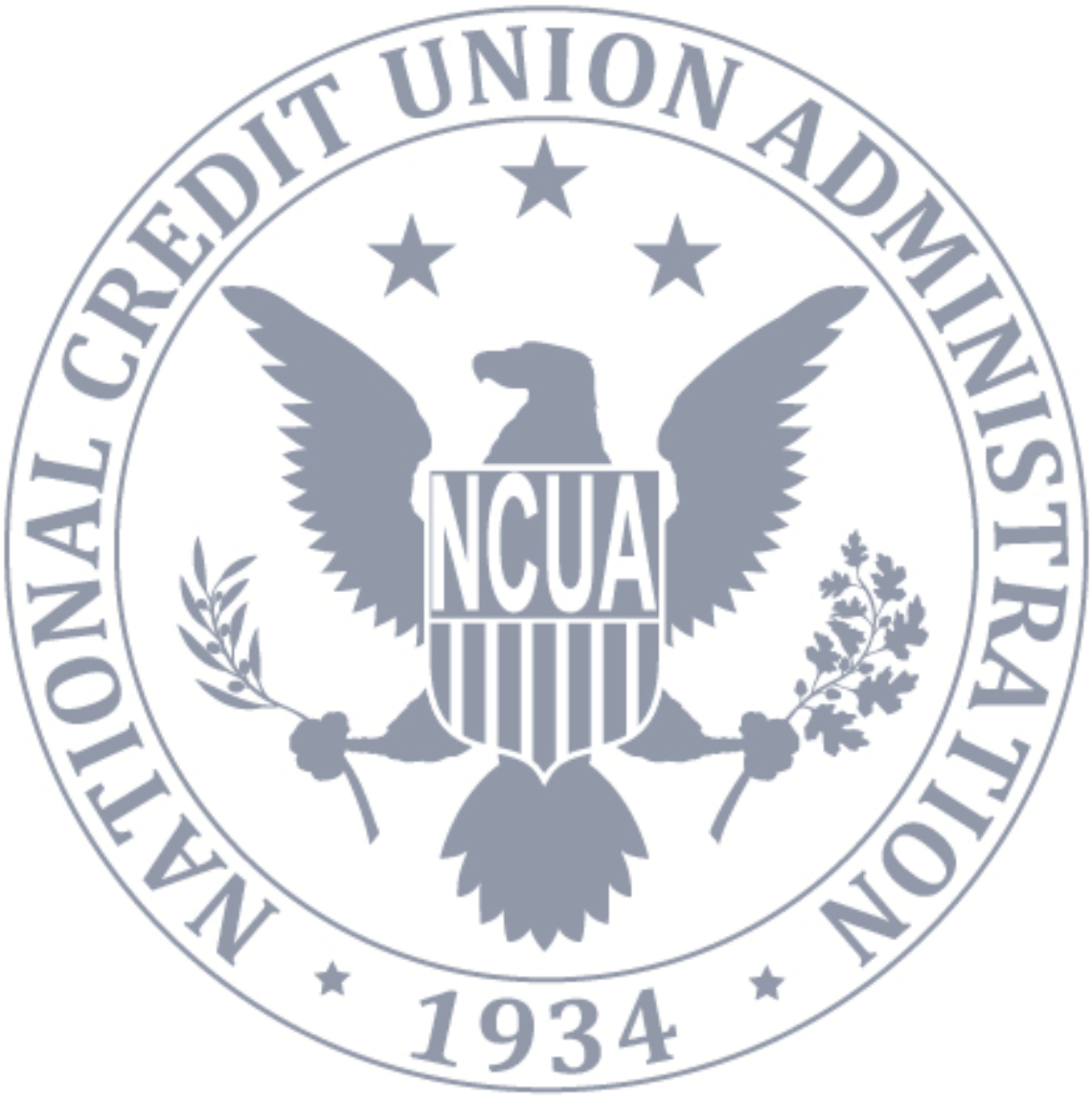
NCUA
National Credit Union Administration

Privacy Impact Assessment for eOPF

Fiscal Year 2018

[This page intentionally left blank]



PIA for eOPF • 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: eOPF

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. 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

The Office of Personnel Management, requires federal agencies to maintain an employee record on each employee in eOPF. These electronic records are used to document an employees federal history. Forms are completed by the employee, certified by OHR and uploaded to the employee's eOPF. The contents of eOPF is documented in OPM's Guide to Recordkeeping. Hard copies are maintain in a lock room for one year.

Intended Use of the PII Collected

To comply with the requirements in 5 CFR Part 293 and OPM's Guide to Personnel Recordkeeping.

Sharing of the PII

eOPF is limited to those whose official duties require such access. Employees have access to his/her eOPF. eOPF documents are shared with the following entities: Office of Personnel Management - Sole owners of eOPF for all federal agencies that utilize eOPF. Retirement and Investigation purposes.National Personnel Record Center (NPRC) - The permanent and performance side of eOPF is submitted to the NPRC when employee separates from federal service.Another Federal Agency - eOPF is transferred electronically if employees transfers to another federal agency. Office of the Inspector General - Access is granted.In accordance to OPM guidelines, immediate supervisors can request limited access to his/her direct reports.

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

eOPF collects electronic copies of employee personnel documents/forms that contain PII data. Documents such as, applications/resume, benefit elections, beneficiary designations, notification of personnel documents, veteran status, background and security certificate, probationary, etc. These documents maintain PII data such as name, SSN, date of birth, home address, SSN, date of birth and home addresses of family members, etc.

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

Data is collected from the following sources:

- Employees – Complete forms electronically through USAStaffing Onboarding or on paper. If paper, OHR scans and upload paper forms to eOPF and electronic documents are transferred to eOPF through USAStaffing Onboarding.
- Comprehensive Human Resources Integrated System (CHRIS) - Information is collected in CHRIS by OHR and transmitted electronically to eOPF.
- Employee Express (EEX) - Benefit elections are processed in EEX by employees and transmitted to eOPF.
- Former Federal Agencies – When an employees transfers from one agency to NCUA, the former sends relevant informmation to NCUA.

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

As custodian of eOPF, OHR is required to safeguard the information that is maintained in eOPF. Here are ways to safeguard eOPF access and use:
Limit Access Logon from a secure government computerPrint only to a secure printer that is in a lock room.Dispose of any printed copies as appropriate.Report any unauthorized access or use of eOPF. Educate users on the importance of securing and dispose of PII data.

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/GOVT-1.

Availability of Privacy Notices

The SORN and PIA for the eOPF 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.

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 7/27/17.

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