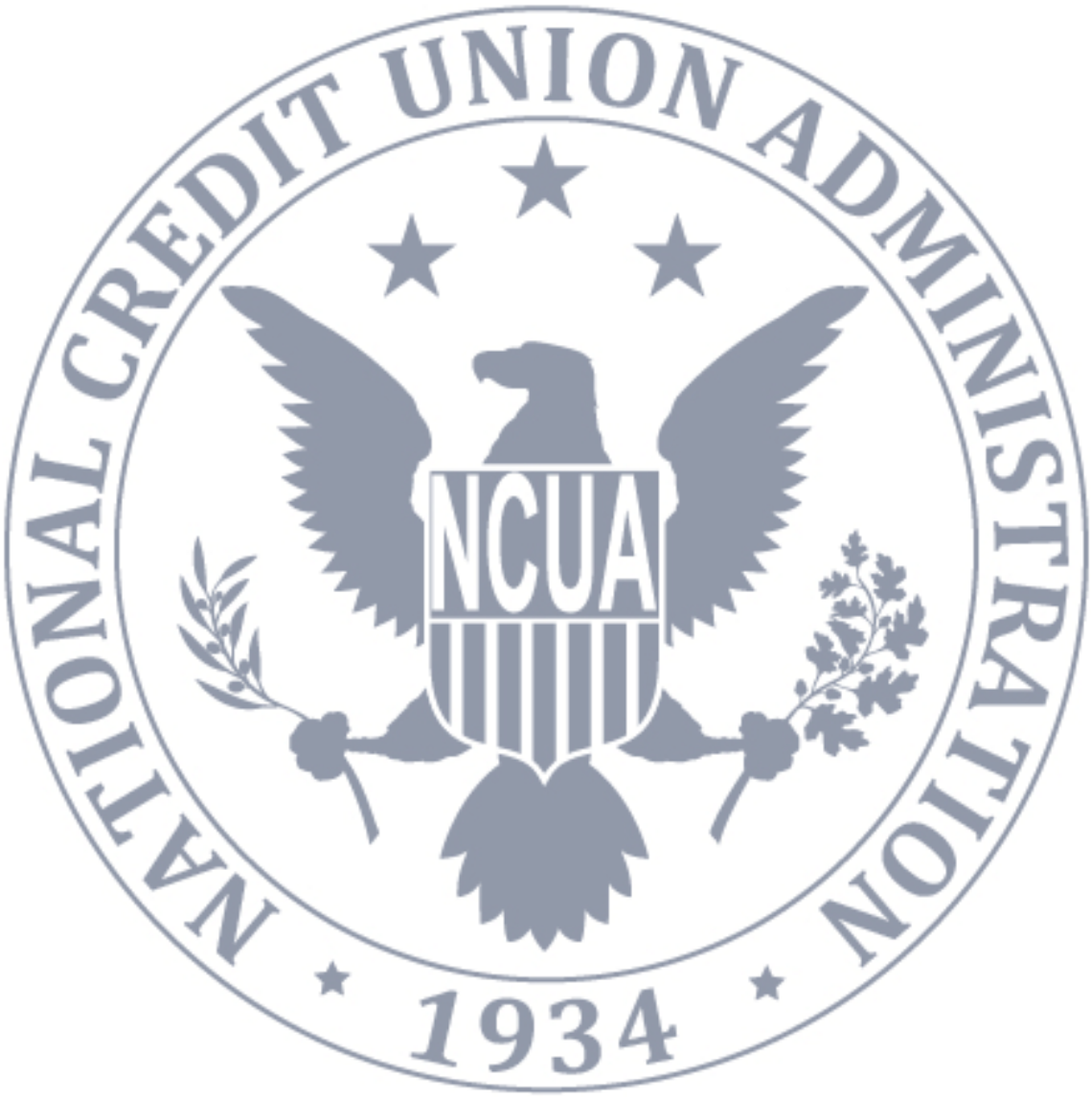
NCUA
National Credit Union Administration

Privacy Impact Assessment for HRLinks

Fiscal Year 2018

[This page intentionally left blank]



PIA for HRLinks • 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: HRLinks

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

HR Links will serve as NCUA repository and authoritative source for employee information. HR Links will collect and maintain PII information for the purpose of time and attendance, payroll, and benefits and retirement processing.
The legal authorities to maintain personnel information and Social security numbers are:

- 5 U.S.C pt. III
- E.O. 9397
- 26 CFR 31.6011(b)-2
- 26 CFR 31.6109-1

Intended Use of the PII Collected

HR Links will be NCUA's authoritative source for capturing PII information on employees. HR Links will use PII information for the following business functions:

- To process personnel actions, time and attendance records and benefit elections for biweekly payroll processing. SSNs are required to interface with GSA Payroll.
- To support processing of NCUA 401K program and debt collection.
- To update employee's Electronic Official Personnel File and generate demographic information required by US Office of Personnel Management (OPM) and Equal Employment Opportunity Commission (EEOC).
- To generate Employee Data File (EDF) for internal agency systems.

Sharing of the PII

NCUA's Office of Human Resources may give access to and/or share information in

HR Links with the following individuals and entities within NCUA:

- NCUA employees – To view their own information, request limited personnel actions and benefit changes and update limited information in their record.
- NCUA managers and timekeepers – For time and attendance reporting and to request personnel actions and approve time and attendance records.
- NCUA HR, HR Liaisons and authorized HR Contractors – To maintain, track and process personnel actions, benefit elections, and performance information. To generate reports such as alpha rosters, demographic data, length of service for workforce planning purposes. HR Liaisons' access be limited to their employee information only.
- NCUA Office of the Chief Financial Officer (OCFO) – To disclose information for debt collections, time and attendance records and payroll reporting.
- NCUA Office of the Chief Information Officer (OCIO) - HR Links will also interface with NCUA network to push employee information to a variety of internal systems as needed.
- NCUA Office of General Counsel – For FOIA processing or legal proceedings.
- Other authorized officials engaged in investigating or settling a grievance or complaint.

HR Links will also interface with GSA for processing payroll, benefit deductions, and the NCUA 401K program.

Information in HR Links will also be shared with the Office of Personnel Management (OPM) to update the Central Personnel Data File (CPDF), the Enterprise Human Resources Integration (EHRI) and the Electronic Official Personnel File (eOPF). Information in HR Links may be shared with other federal agencies requesting information on employees that are seeking employment elsewhere in federal government, or when otherwise necessary and appropriate (such as to sharing demographic statistical reports for required annual MD-715 reporting to the Equal Employment Opportunity Commission (EEOC)).

IBM will also have access to the system as necessary to carry out their responsibilities as the HR Links system provider.

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

HR Links will collect and maintain personal information about NCUA employees, including full name, Social Security Number (SSN), employee family SSNs, date of birth (DOB), home address, home telephone number, personal email address, employee identification number (EID), ethnicity/race, handicap information, employee disciplinary data, gender, marital status, education history, benefits information, military status, time and attendance records and other pertinent information related to supporting human resources information and time and attendance processing.

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

Information collected in HR Links will be provided by the employee and/or other federal entities and updated by NCUA's Office of Human Resources. Personnel actions are authorized by office directors and approved by Office of Human Resources. Time and Attendance is approved by immediate supervisors.

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

Users of HR Links are authorized personnel staff that has a need-to-know the information contained in HR Links in order to carry out their duties. User access to the data is determined based on the user's job requirements. Access to the system is requested by supervisor and approved and granted by HR Links Administrator. Any related paper records will be appropriately safeguarded and maintained pursuant to NARA requirements.

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 HRLinks 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 9/5/2017.