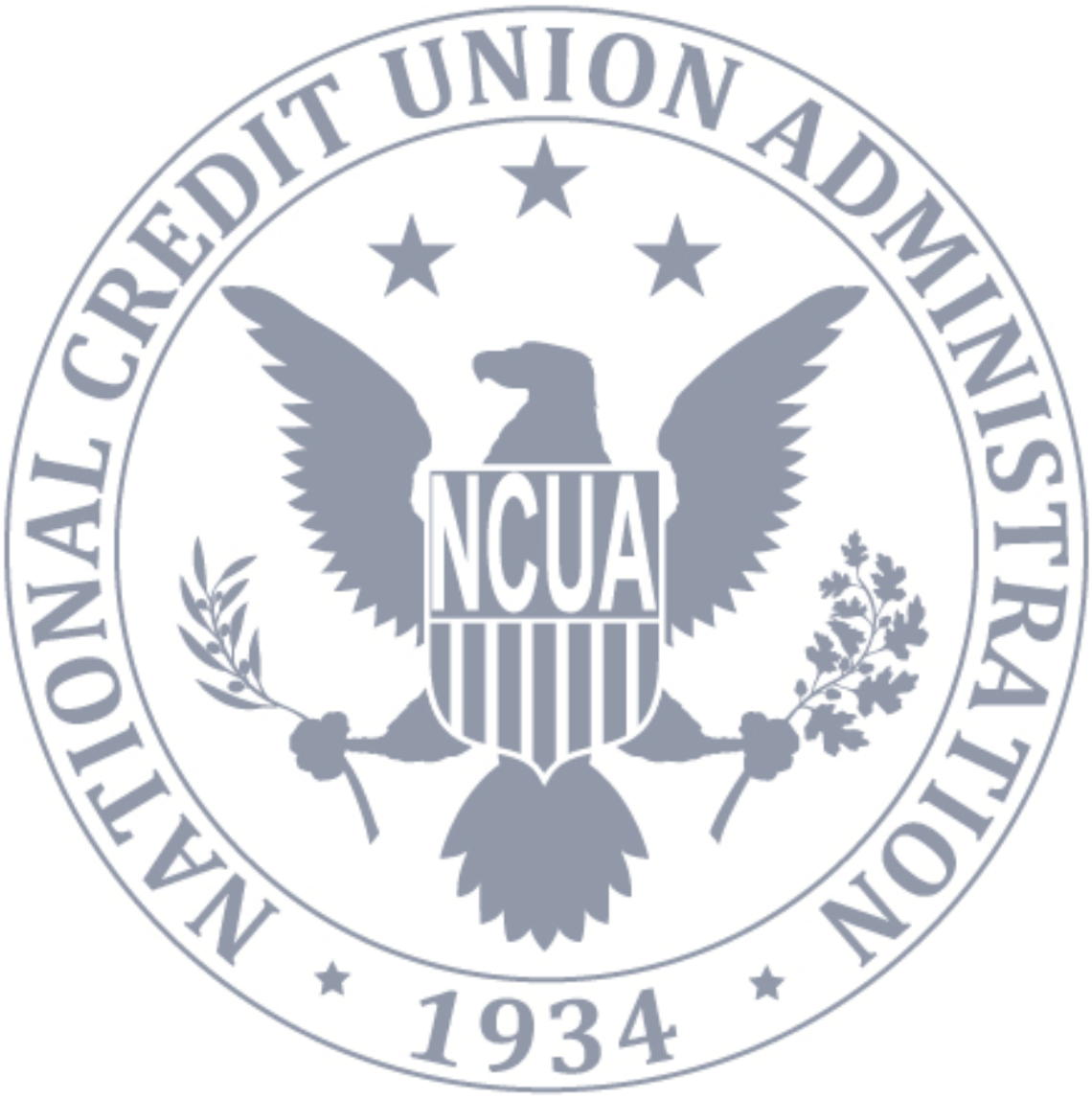
NCUA
National Credit Union Administration

Privacy Impact Assessment for Insurance Information System (IIS) (GENISIS / FOMIA)

Fiscal Year 2018

[This page intentionally left blank]



PIA for Insurance Information System (IIS) (GENISIS / FOMIA) • 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: Insurance Information System (IIS) (GENISIS / FOMIA)

NCUA Office Owner: Office of Credit Union Resources and Expansion (CURE)

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

GENISIS

- NCUA employees - PII collected is to identify which NCUA employee is assigned to process the submitted request, and is used in the FOM Dashboard to inform a credit union as to who is processing their request.
- Interested parties (credit unions, subscribers/organizers for proposed credit unions, and the public) - PII collected (if deemed needed) is to identify the person that a request for action is being completed on. For example, if a credit union member submitted a share insurance question, the submitter's name would potentially be typed in the Reference field in the GENISIS log in order to identify this log was submitted by that person.

FOMIA

- Interested parties:
  1. Credit unions - PII collected is to identify what credit union employee submitted the request, as indicated on NCUA Form 4015-EZ and required by NCUA's Field of Membership and Chartering Manual (Chapter 2, Section IV.B.3).
  2. Public (field of membership groups) - PII collected is to identify what field of membership group representative submitted the request to the credit union, as required by NCUA Form 4015-EZ (that a letter from the group requesting credit union service must be attached).

Intended Use of the PII Collected

GENISIS

- NCUA employees - PII facilitates NCUA in assigning and tracking work within CURE 's Division of Consumer Access and Division of Consumer Access-South. When a new log is created in GENISIS, a reviewer is assigned to the log.

The reviewer is the first and last name of an authorized NCUA employee. For historical and report running purposes, all logs created in GENISIS are kept. Therefore, a reviewer's first and last name will be associated to that log as long as that log is kept.

- Interested parties - PII facilitates NCUA in identifying and tracking (if needed) which person goes with which request for action regarding work within CURE 's Division of Consumer Access and Division of Consumer Access-South. When a new log is created in GENISIS as the result of receiving a noncredit union request, the first and/or last name of the submitter could be entered into the log (into the Reference field). For historical and report running purposes, all logs created in GENISIS are kept. Therefore, a submitter's first and/or last name will be associated to that log (if entered into the log's Reference field) as long as that log is kept.

FOMIA

- Interested parties - PII documents the credit union's compliance with the Field of Membership and Chartering Manual that requires the name and title of the credit union board authorized representative be identified. A person's PII is entered into the FOMIA system by the credit union, upon a credit union being granted access to the FOMIA system. For historical and report running purposes, all requests are kept. Therefore, PII associated to that request will exist as long as the request data is kept.
- Public (field of membership groups) - PII documents the credit union's compliance with the Field of Membership and Chartering Manual that requires the credit union obtain a letter from an authorized representative of the group. A person's PII is entered into the FOMIA system by the credit union, upon a credit union submitting a request through the FOMIA system. For historical and report running purposes, all requests are kept. Therefore, PII associated to that request will exist as long as the request data is kept.

Sharing of the PII

GENISIS

PII is only shared with other NCUA employees authorized to use the system, as well as any NCUA staff member that a report containing PII would be shared with (generally just CURE management).

FOMIA

- NCUA employees - no PII is shared as it is not collected.
- Interested parties:
    1. Credit Unions – as FOMIA flows into GENISIS, PII is only shares with other NCUA employees authorized to use the system, as well as any NCUA staff member that a report containing PII would be shared with

(generally just CURE management).
2. Subscribers/organizers for proposed credit unions – no PII is shared as it is not collected.
3. Public (field of membership group) – as FOMIA flows into GENISIS, PII is only shared with other NCUA employees authorized to use the system, as well as any NCUA staff member that a report containing PII would be shared with (generally just CURE management).

GENISIS data and CU Online data flow into the FOM Dashboard, a cloud-based Salesforce environment via web service, the following PII would be shared with one (per credit union) approved designed credit union representative:

• NCUA employee's first and last name assigned to process a request submitted by the credit union.
• Any submitter's first and/or last name, if deemed needed to identify that person with the request for action.

The FOM Dashboard is only accessible to credit unions – to one designated registered user per credit union. It is not available to the public (a subscriber/organizer for a proposed credit union, a credit union member, a field of membership group, etc.).

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 following PII is collected on NCUA employees and interested parties, as described below.

GENISIS

- NCUA employees (those with permission to use this system - is around 20 individuals) - PII includes the employee's first and last name.
- Interested parties (credit unions, subscribers/organizers for proposed credit unions, and the public) - PII can include, if deemed needed, the submitter's first and/or last name and would be manually typed into the "Reference" field by an authorized NCUA employee.

FOMIA

- NCUA employees - no PII is collected.
- Interested parties:
    1. Credit unions - PII includes the credit union employee's first and last name, position/title at the credit union, and work phone number.
    2. Subscribers/organizers for proposed credit unions – no PII is collected.
    3. Public (field of membership group) - PII includes the group representative's first and last name, position/title at the group, and work phone number.

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

NCUA employees-from NCUA's employee records (IT system).

CU Board or FOM Group Authorized Representatives-manually from CUs. Proposed CU Subscriber/Organizer or Person from Public-manually from submitted request.

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

GENISIS – only authorized NCUA employees are given access to this system, on an NCUA issued computer with PIV card authentication.

FOMIA – only authorized Federal Credit Unions (multiple common bond charters) are given access to this system with the use of an NCUA generated pin. The pin is generated by NCUA using a protected algorithm. It is 11 to 14 characters. It is case sensitive and is composed of upper case, lower case and numbers. It does not automatically expire but it is at NCUA's discretion as to when and how often to re-generate them. It is normally done on demand when requested by CURE management or the credit union. The pin is never reused, as the PIN generation algorithm uses a combination of current system date/time stamp that changes every time it is regenerated.

FOM Dashboard – only authorized Credit Unions are given access to this system with an NCUA generated user name and a password that is established by the designated registered user.

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 the Insurance Information System (IIS) (GENISIS / FOMIA) is 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 6/8/17.

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