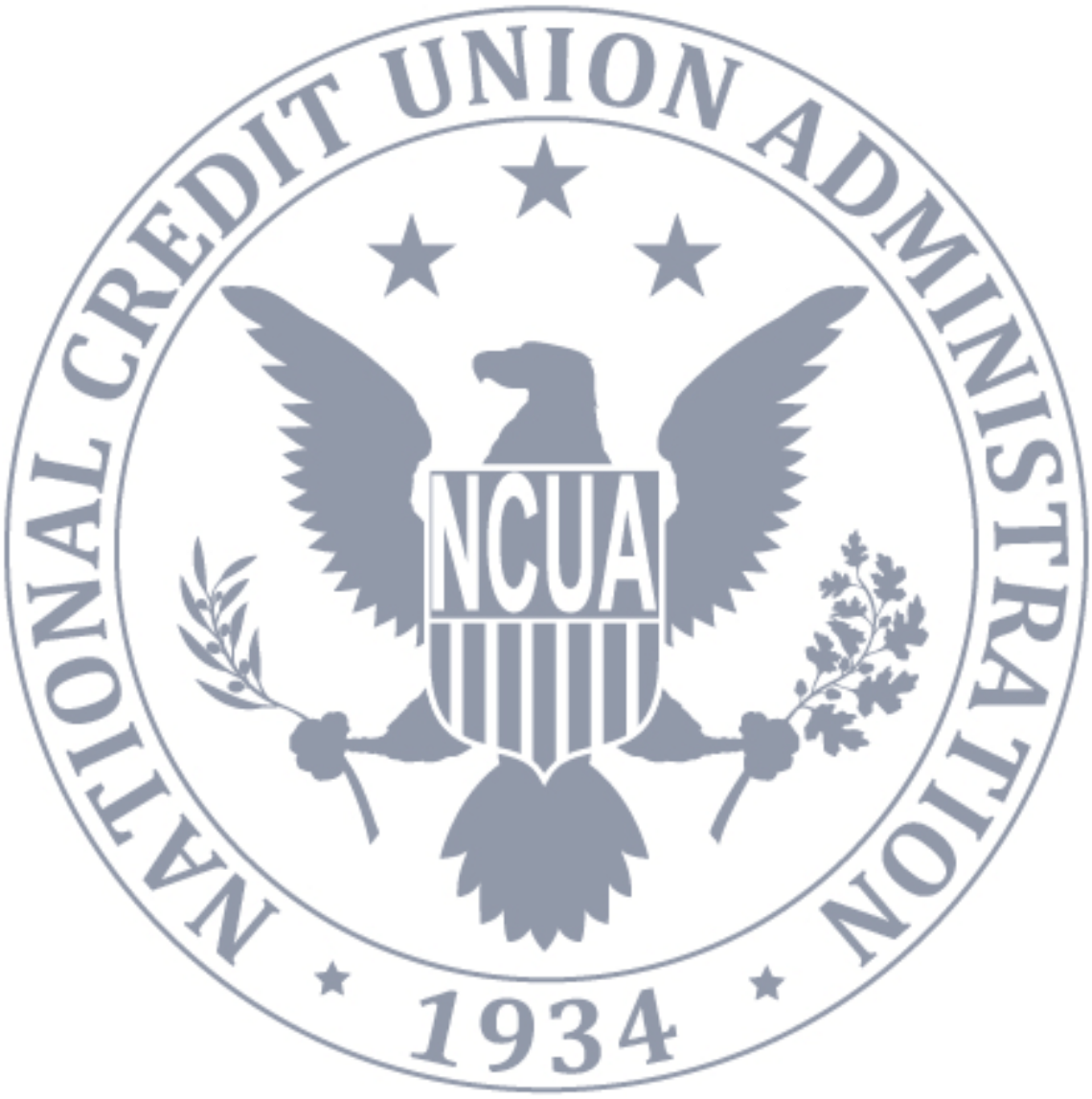
NCUA
National Credit Union Administration

Privacy Impact Assessment for Integrity

Fiscal Year 2018

[This page intentionally left blank]



PIA for Integrity • 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: Integrity

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

5 U.S.C. App. (Ethics in Government Act of 1978); E.O. 12674 (as modified by E.O. 12731).

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

All records are maintained in accordance with the requirements of the Ethics in Government Act of 1978 and the Ethics Reform Act of 1989, as amended, and Executive Order 12674 as modified and OGE and agency regulations thereunder. These requirements include the filing of financial status reports, reports concerning certain agreements between the covered individual and any prior private sector employer, ethics agreements, and the preservation of waivers issued to an officer or employee pursuant to section 208 of title 18 and certificates of divestiture issued pursuant to section 502 of the Ethics Reform Act. Related records are required to assure compliance with these acts and to preserve and promote the integrity of public officials and institutions.

There are two government wide SORN's

- OGE/GOVT–1 (PDF) is a system of records containing public financial disclosure reports and other name-retrieved ethics program records.
- OGE/GOVT–2 (PDF) is a system of records containing confidential financial disclosure reports, including OGE Form 450, OGE Optional Form 450-A, and agency supplemental or alternative confidential report forms.

Intended Use of the PII Collected

Information is collected via web interface and stored on secure servers maintained by the Office of Government Ethics for access by authorized personnel. Those who are obligated by statute to file (Filers) will prepare the report themselves or appoint representatives to enter the information on their behalf.
NCUA ethics officials use the information Filers provide to determine compliance with applicable Federal laws and regulations and to identify and resolve any potential

conflicts of interests between an employee's official duties and private financial interests and affiliations.

Sharing of the PII

Personal and financial information collected is treated as private and sensitive and is limited to select individuals. Filers are added to Integrity by NCUA Ethics officials before user access. The NCUA Alternate Designated Agency Ethics Official initially assigned report reviewers one or more "roles" that correspond with the appropriate level of data access privilege. Data access is limited to only the information needed to perform assigned duties. The financial disclosure report may be viewed by the report Filer and the appropriate NCUA reviewing official assigned to that particular filer. Integrity reviewers and certifiers for NCUA include the central office ethics officials. Additionally, staff within OCIO may have limited access to perform technical support. A filers report data may be created/modified by the following:

- The filer's assistant can create/modify filer data before the filer submits a report into the review process – once submitted, an assistant can only view the filer's data.
- A filer can create or modify filer data any time before it has been submitted for final ADAEO review – once submitted for that final review, a filer can only view his/her data.
- Reviewers are allowed to modify filer data in a report.
- Reviewer's can add comments to a report. Further, comments entered by a reviewer cannot be modified or deleted by another reviewer.

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

NCUA's office of General Counsel is conducting a Privacy Impact Assessment (PIA) for the Integrity System. Integrity is a web-based software program developed by the Office of Government Ethics to allow individuals via electronic means to complete, sign, and file financial disclosure reports OGE 278 (Executive Branch Public Financial Disclosure Reports). The financial disclosures are reviewed by NCUA ethics officials to identify and resolve possible conflicts of interest between a filers financial interest and their official duties. A PIA is being created because Integrity collects and stores filer

personally identifiable information.

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

The data is collected from required filers and is collected via the internet

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

Access to the FDM system by either filer or reviewer/certifier is protected through the use of PIV card and pin number.
Pursuant to the National Archives and Records Administration General Records Schedule for ethics program records, these records are generally retained within the Integrity system for a period of six years after filing. Destruction is by electronic deletion performed by Integrity.
Regarding FDM system security, please see the information below gathered from the Integrity Website.
Implements Guidance of:

- Federal Information Security Management Act (FISMA)
- National Institute of Science and Technology (NIST) Special

Publications

- Office of Management and Budget (OMB)

Security Features

- 256-bit data encryption—banking industry standard
- Limited-access system
- Role-based permissions
- Only the Filer, any designees, and authorized reviewers see Filer

data

- Independent verification and validation of security controls
- Continuous security monitoring

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 OGE/GOVT-1.

Availability of Privacy Notices

The SORN and PIA for the Integrity 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 8/1/17.

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