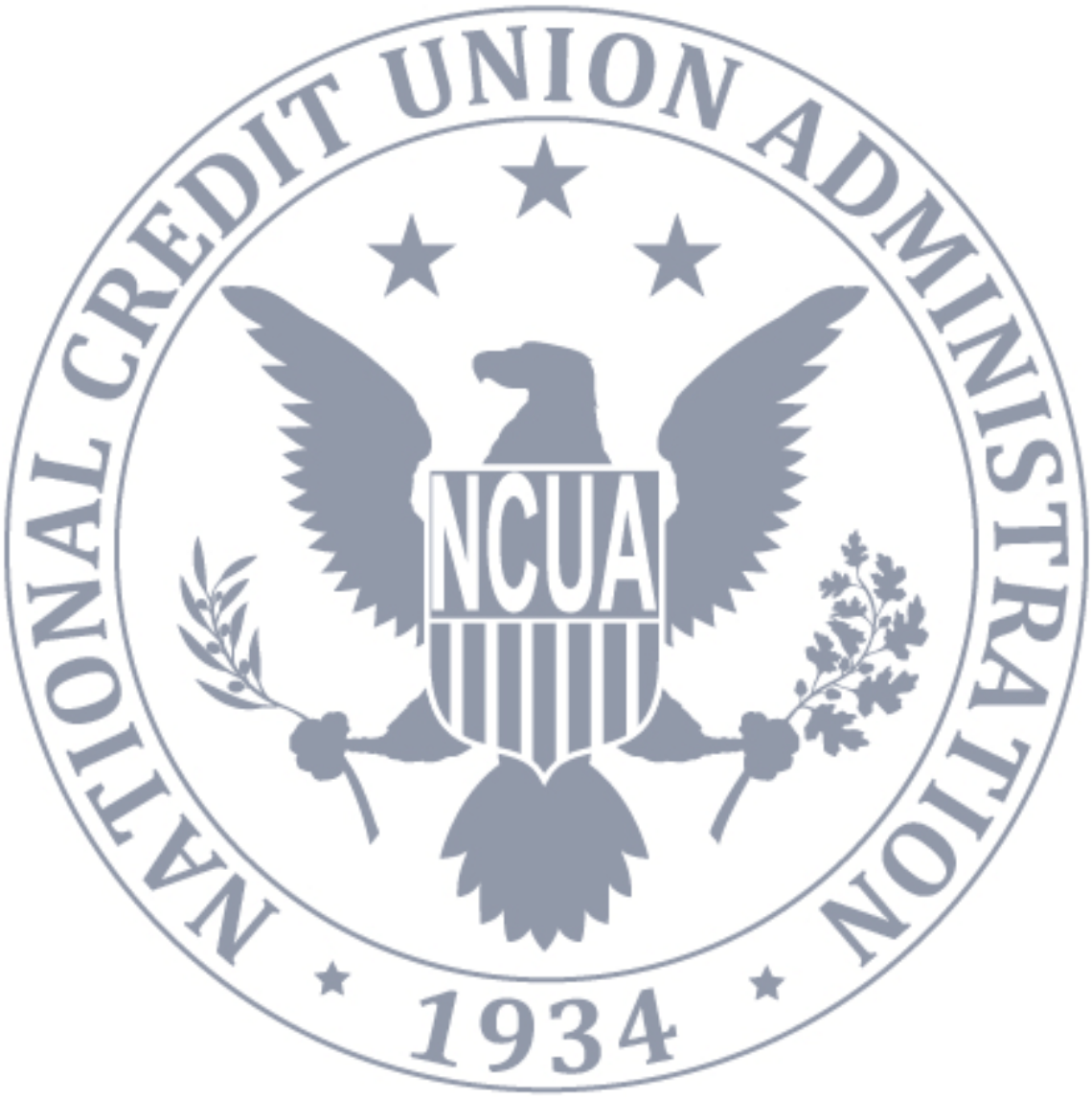
NCUA
National Credit Union Administration

Privacy Impact Assessment for Financial Management Disclosure (FDM)

Fiscal Year 2018

[This page intentionally left blank]



PIA for Financial Management Disclosure (FDM) • 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: Financial Management Disclosure (FDM)

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.

Intended Use of the PII Collected

Information is collected via web interface and stored on secure servers maintained by the Department of the Army 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 FDM 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 (i.e., supervisor, certifying official) assigned to that particular filer.

FDM reviewers and certifiers for NCUA include the central office ethics officials, the ethics officials for each NCUA region, the general counsel for the NCUA Inspector General Office. 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 can never create or 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 Financial Disclosure Management System (FDM). FDM is a web-based software program developed by the Department of the Army to allow individuals via electronic means to complete, sign, and file financial disclosure reports OGE 278 (Executive Branch Public Financial Disclosure Reports) and OGE 450 (Executive Branch Confidential 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 FDM collects and stores filer personally identifiable information.

NCUA originally used the FDM system to process both OGE form 278 and OGE 450. However, because of the implementation of the Integrity System (used to process OGE 278), we will only be using FDM to process OGE 450 for the 2016 filing season and beyond. NCUA may also use FDM infrequently for historical OGE 278 filing information.

FDM collects the following information: Financial information such as salary, dividends, retirement benefits, interests in property, deposits in a bank and other financial institutions; information on gifts received; information on certain financial liabilities and certain financial assets, information about positions as an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, company, firm, partnership, or other business, non-profit organization, labor organization, or educational institution, information about non-Government employment agreements, and the continuation of payments by a non-Federal employer. Please note that when information not specifically required to be reported by the disclosure report or statute is found in the Filers' records, Filers will be notified and asked to delete such 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 NCUA employees designated by a supervisor as a 450 filer.

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 a username and password. NCUA/FDM are currently in the process of requiring use of PIV card for access to the FDM system.

Pursuant to the National Archives and Records Administration General Records Schedule for ethics program records, these records are generally retained within the FDM system for a period of six years after filing. Destruction is by electronic deletion performed by FDM.

Regarding FDM system security, please see the Questions and Answers below gathered directly from the FDM Website.

Q: What assurance do filers have that their information can't be intercepted over the Internet? (Communication security)

A: FDM is a secure, web-based application. All communications between the FDM servers and the user's desktop/laptop computers are secure - making it virtually impossible for someone to “snoop” on the communications.

Q: What assurance do filers have that FDM's servers are protected from hackers? (Logical intrusion -- Hacker security)

A: FDM is hosted on a server that has been hardened using current DISA guidance. Ports and services that are not needed have been removed from the operating system. Servers are patched on a regular basis or as updates are provided. Hardware firewalls and Intrusion Detection Systems (IDS) are monitoring and blocking unauthorized connections outside the enclave. The servers use current anti virus software to check for viruses in real time and check all files weekly. Virus definitions are set to automatically download nightly. Logs are checked for unauthorized access or server problems on a routine basis.

Q: What assurance do filers have that FDM's servers are protected from physical intrusion? (Physical security)

A: The servers are located in secured server rooms. The building is guarded IAW local security procedures. There is no access without a government issued building access pass, or without an escort by a person with a building pass. Access is granted to government sponsored individuals only.

Data backups are routinely performed and stored on tapes and/or a server in another Government facility at a different location. Security for those servers and for the server rooms is comparable to the primary server location. All server rooms used are climate controlled with both air conditioning and humidifiers to control heat and static electricity.

Q: What happens in the event of a compromise of a Filer's personal financial information?

A: The FDM Program Office will initiate action in accordance with Department of Defense policy, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, https://dpcld.defense.gov/Portals/49/Documents/Privacy/PII_Memo_Safeguard.pdf (5 Jun 2009).

Q: What redress is available in the event of a compromise of personal data?

A: The person who suffered the compromise may report the matter to the Army Privacy Office,https://www.rmda.army.mil/privacy/RMDA-PO-Infractions.html, and the FDM Program Office for investigation.

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-2.

Availability of Privacy Notices

The SORN and PIA for the Financial Management Disclosure (FDM) 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 8/3/17.

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