



**NCUA**  
National Credit Union Administration

# Privacy Impact Assessment for CyberGrants: Chartering Proof of Concept

---

Fiscal Year 2019

[This page intentionally left blank]





## PIA for CyberGrants: Chartering Proof of Concept • FY2019

### Table of Contents

---

About this Document .....	2
Basic Information about the System .....	2
Authority .....	3
Purpose Specification and Use Limitation .....	3
Minimization.....	4
Individual Participation.....	5
Quality and Integrity .....	5
Security .....	5
Transparency.....	5
Accountability.....	6
Approval.....	7





## 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.<sup>1</sup> Completion of a PIA is a precondition for the issuance of an authorization to operate.<sup>2</sup>

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:** CyberGrants: Chartering Proof of Concept

**NCUA Office Owner:** CURE

**System Manager:** [REDACTED]

---

<sup>1</sup> 44 U.S.C. § 3501, note; Pub. L. 107-347, § 208(b).

<sup>2</sup> OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).



## 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.*

### 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

This information is collected in the Proof of Concept (POC) for the (7) individuals who are responsible for the formation of the credit union. The Federal Credit Union Act requires that (7) or more natural persons present to NCUA for approval a sworn organization certificate.

NCUA will have ongoing communication with these (7) individuals as the Office of Credit Union Resources and Expansion (CURE) guides each organizing group through the chartering process.

### Intended Use of the PII Collected

If an organizing group successfully meets the requirements for the POC, they will receive an invitation to submit a formal charter application. The PII captured in the POC is only used as a method for communicating with all of the subscribers concerning the status of POC submission.



## Sharing of the PII

The PII is not shared with any other entities or organizations.

## 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 PI Collected

The PII being collected include the Name, Telephone Number, and Email Address of seven individuals involved in the formation of a new credit union. These individuals are referred to as Subscribers.

## 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 one of the seven individuals (Subscribers) and it is collected through the CyberGrants software for the Chartering Proof of Concept.

## 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

Information submitted to CURE in the POC is only accessible by CURE staff with chartering-related job responsibilities and a CyberGrants user account. CURE's Director of Operations is responsible for granting staff with access to a user account. The user accounts contain login rules which require staff to use a combination uppercase, lowercase, numeric, and special characters. In addition, the login credentials expire every 60 days.

## 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 CyberGrants: Chartering Proof of Concept 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.<sup>3</sup>

## 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 6/7/19.

---

<sup>3</sup> 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.