NCUA
National Credit Union Administration

FY 2017

Privacy Impact Assessment for NCUA General Support System (GSS)

[This page intentionally left blank]

PIA for NCUA General Support System (GSS) • FY 2017

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 questions on the PIA form correspond with the Fair Information Practice Principles.[3]

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: NCUA General Support System (GSS)

NCUA Office Owner: OCIO

System Manager: [redacted]

[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).
[3] The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that serve as the foundation of all privacy laws and policies in the federal government and many U.S. states and foreign nations, recently re-published by the Office of Management and Budget in OMB Circular A-130, *Managing Information as a Strategic Resource* (2016).

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

NCUA OPIs use OPI-owned applications that reside on the GSS computing platform to collect, create, maintain, and/or distribute the PII of NCUA employees, state examiners, credit unions, and contractors. The NCUA GSS provides the computing platform for NCUA OPI applications. The platform includes all IT hardware, communications, network storage, central databases, and operating systems. The NCUA GSS is reliant on the OPI application data owners to complete PIAs to document the information collection reason, as required.

Intended Use of the PII Collected

NCUA OPIs use OPI-owned applications that reside on the NCUA GSS. The NCUA OPI application Privacy Impact Assessments (PIAs) describe the intended agency use for PII that is collected, created, maintained, and/or distributed.

Sharing of the PII

Other than NCUA employees and contractors, State Supervisory Examiners have access to the PII. The Senior Agency Official for Privacy (SAOP) has primary oversight responsibility for the Privacy Program, particularly privacy management policies and processes. Offices that control the data (offices of primary interest) are responsible for assuring proper use of data in the system. Related procedures are governed by internal

policies and directives. Examples of such directives include 3226.2 NCUA Privacy Program, 4900.02, Guidance on Release of Credit Union Information, 1200.15, Rules and Consequences for Safeguarding Personally Identifiable Information, 13500.09, Security of External Party's Documentation, and 13500.11, Information Sharing with State Supervisory Authorities.

The NCUA GSS has the following external connections:

NAME	EXTERNAL ORGANIZATION	BUSINESS USE/DATA PROVIDED
CHRIS	GSA	CHRIS is used for payroll processing. NCUA HR staff input employee data into CHRIS. CHRIS data is considered the master payroll file. NCUA then pulls data from CHRIS into its SAP payroll processing system.
ePerformance	Northrup Grumman	ePerformance is used for employee performance appraisals. Managers input employee performance data into the system. HR then pulls the data and sends to the Office of Personnel Management (OPM).
CONCUR	GSA	CONCUR is NCUA's travel management system. Name, credit card numbers, banking information, travel reservations/itineraries are included in the system.
Pay.gov	FRB/Treasury	Pull daily reports of members who have made payment on pay.gov for debts owed to the liquidation estates.
DELPHI	DOT-FAA	DELPHI is used for processing payments to vendors. Vendors submit invoices with pay instructions (e.g., EIN, Bank Account, etc.). NCUA staff work with vendors to send data to Shared Service Providers for payment processing.
e-Delivery	OPM	eOPF collects electronic copies of employee personnel documents that contain PII data. Documents such as, applications/resume, benefit elections, beneficiary designations, notification of personnel documents, veterans

status, background and security certificate, probationary, 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

NCUA Offices of Primary Interest (OPIs) use personally identifiable information (PII) and/or sensitive data in the regular course of business. The NCUA OPIs own and operate various applications on the NCUA General Support System (GSS) that collect, create, maintain, and/or distribute PII.

PII pertaining to NCUA employees, state examiners, credit unions, and vendors may include, but is not limited to, the following:
- SSN
- Bank Account and Credit Card Number(s)
- Driver's License Number(s)
- Email Address(es)
- Biometric Data
- Medical History
- Family Member Names
- Military History
- Workmen's Compensation History
- Home Address
- Education and Training History
- Grievance History
- Home/Cell Telephone Number(s)
- EEO History
- Employment History
- Other Family Member Information
- Employment Evaluations
- Security Screening Information
- Credit Ratings and Credit History
- Salary Information
- Birth date / Age
- Password(s) and PIN(s)
- Gender / Race / Citizenship

- Picture

Sensitive credit union-related information collected may include, but is not limited to, the following data:
- CAMEL Code
- Member SSNs
- Member Identifying Information
- Credit Card Information
- Officials' Personal Information
- Member Location Data
- Tax ID Numbers (EIN)
- Bank Account 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

This system provides opportunity for individual 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

NCUA OPIs use OPI-owned applications (i.e., file shares and databases) that reside on the NCUA GSS to collect PII pertaining to NCUA employees, state examiners, credit unions, and vendors.

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

The NCUA GSS employs extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. The security measures include access control, configuration planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

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 sytem, a SORN is not required.

Availability of Privacy Notices

The SORN and PIA for NCUA General Support System (GSS) 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 FIPPs

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 FIPPs.

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.[4]

[4] 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 the Senior Agency Official for Privacy on 7/24/17.