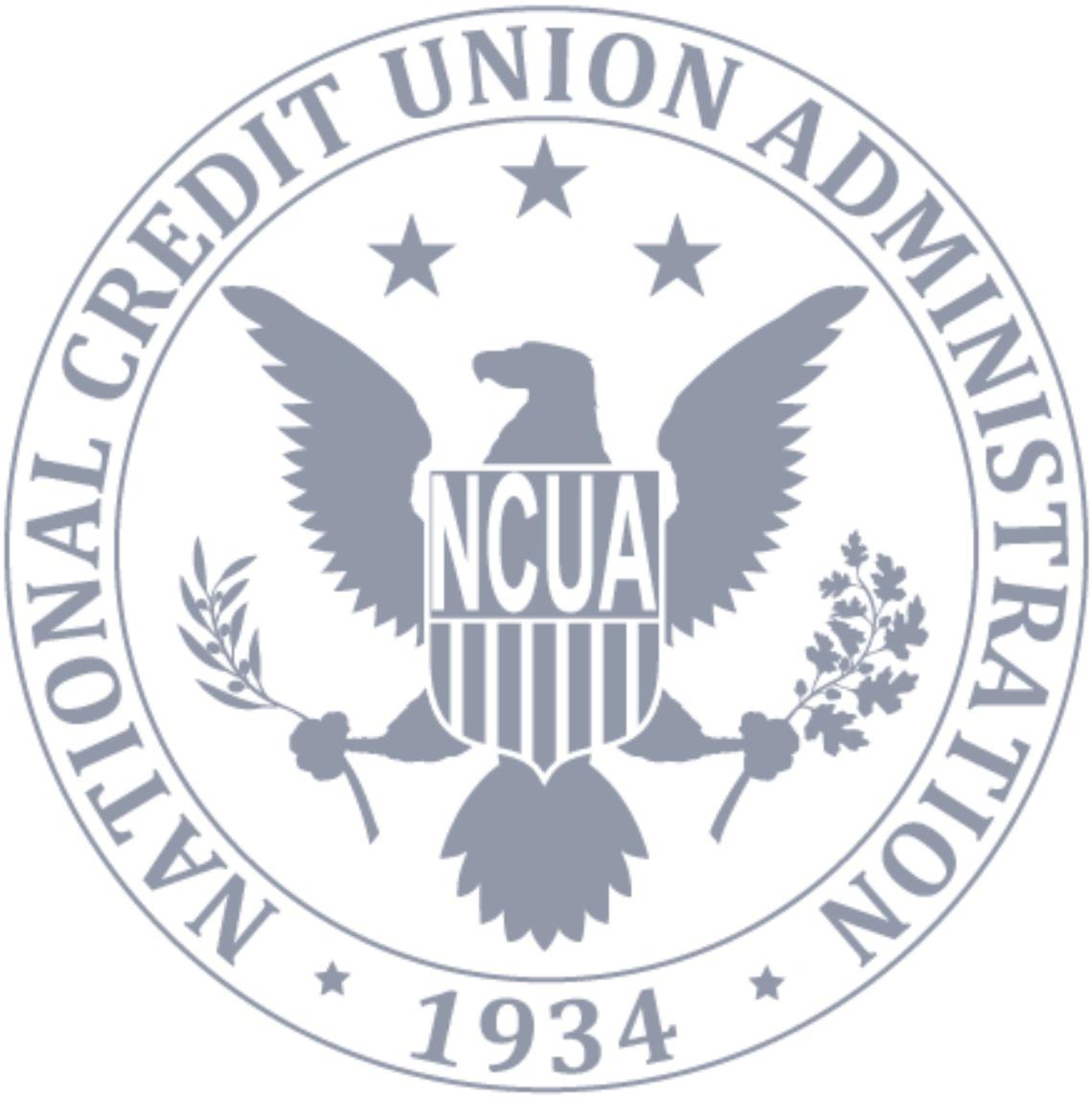
NCUA
National Credit Union Administration

Privacy Impact Assessment for ITSM - Service Now

Fiscal Year 2018

[This page intentionally left blank]



PIA for ITSM - Service Now • 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: ITSM - Service Now

NCUA Office Owner: OCIO

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.; 44 U.S.C. § 3551 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

ServiceNow is an end-to-end IT Service Management system through a cloud-based platform. OCIO utilizes ServiceNow platform to modernize the Service (Help) desk and the reason for collecting these information is to enable the service desk staff to contact the user, know their location, and associate tickets and assets with users.

Intended Use of the PII Collected

ServiceNow is used by OCIO to assist NCUA community with Incident (Ticket) management, self-service portal, knowledge base, and help desk reports. Our goal is to provide methods above to drive efficiencies to quickly identity and resolve IT issues faster and increase satisfaction.

Sharing of the PII

Only the NCUA employees and OCIO contractors have access to the information contained in ServiceNow.

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 information contained in the active directory is synced with ServiceNow therefore information such as username, first and last name, Employee ID, phone number(s), location, and email addresses will be displayed.

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

End-users: When an individual contacts the Service Desk via phone, they speak to a Service Desk analyst who opens a ticket regarding the user's situation and manually enters information that the individual provides over the phone. When an individual submits a ticket via One Stop, they can either select from the top 7 issue items or type in their issues in the description field.

When an individual contacts the Service Desk via email, they describe the issues they are having in the body line of an email. To capture emails to convert them to a ticket, we have a email forwarding rule setup in ServiceNow that any email sent toServiceDesk@ncua.gov will generate a call record which will then be triaged by the service desk analyst to create an incident or a request ticket.

The Active Directory: ServiceNow pulls the data from Active Directory, which contains the official record of current employees and contractors. So when the analyst creates a ticket and types in the user's first name and last name, the information in the AD gets populated in the system. The Active Directory contains information that was originally provided by the office that the employee belongs to via Employee Enter process (e.g., the employee's name was provided by the employee when she started working at NCUA), and information about the individuals, such as email address, office room number, and office phone number, that is created by through routine administrative onboarding processes.

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

ServiceNow is a FEDRAMP certified solution that goes through rigorous security assessment framework. Security is build into all levels of functionality and includes roles and access control rules and audit logs of user interactions. NCUA users use their PIV card to access ServiceNow using NCUA-managed ADFS Single Sign-on.

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 SORN and PIA for the ITSM - Service Now 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 9/19/17.

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