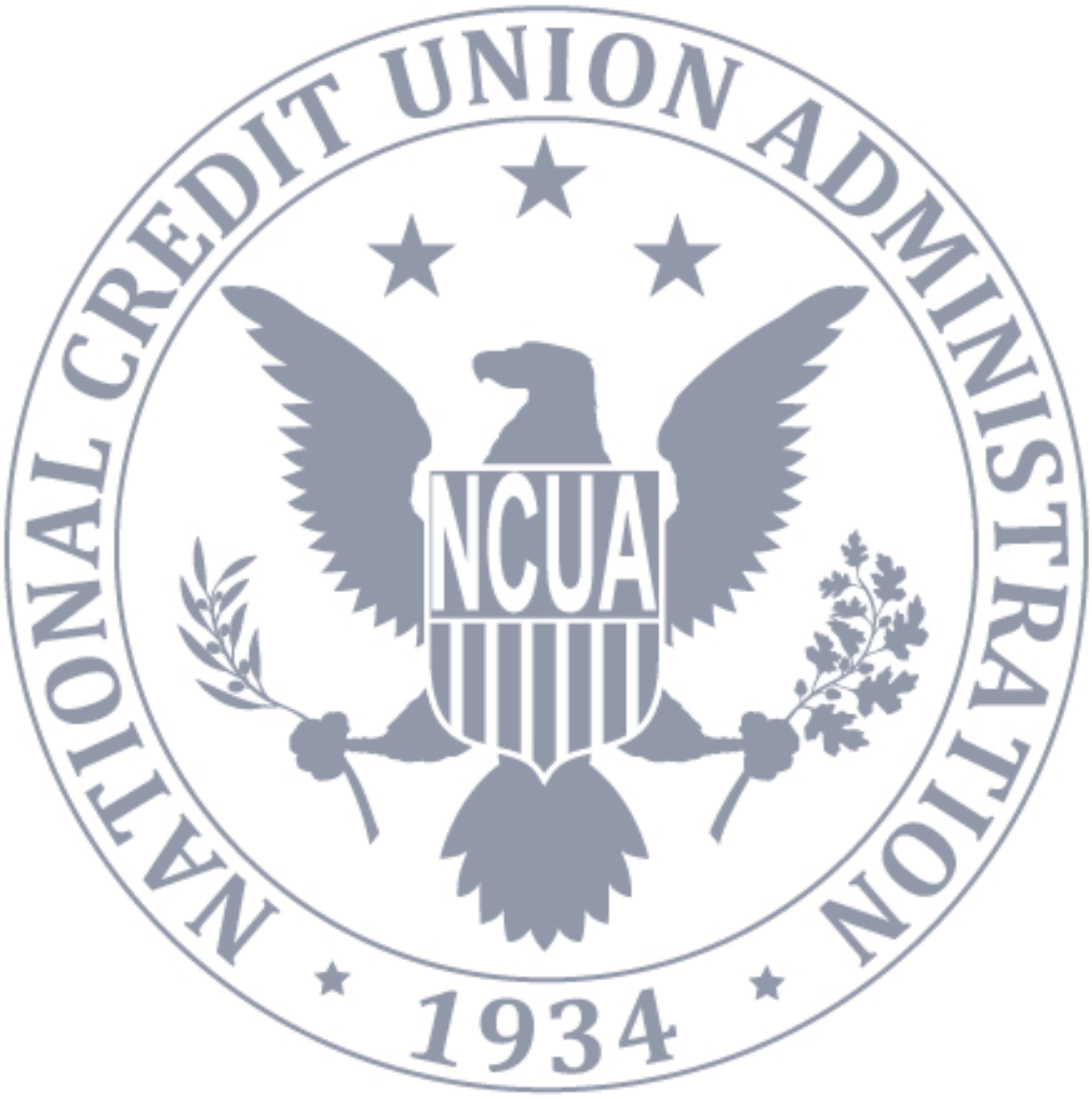
NCUA
National Credit Union Administration

Privacy Impact Assessment for Physical Access Control System (PACS)

[This page intentionally left blank]



PIA for Physical Access Control System (PACS) • 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: Physical Access Control System (PACS)

NCUA Office Owner: OCSM

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. Chapter 73 (Suitability, Security, and Conduct); 5 U.S.C. § 7531-33 (National Security); Executive Order 10450 (Security requirements for government employment); Executive Order 13526 and its predecessor orders (National Security Information); Ho

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

To assist NCUA in securing and regulating physical access to NCUA facilities. For the purposes of public safety in NCUA facilities, internal and external investigations, crime prevention and to assist law enforcement agencies in criminal prosecutions. To address internal personnel, suitability and security clearance issues, and potential insider threats.

Intended Use of the PII Collected

For NCUA to secure and regulate physical access to NCUA facilities. To promote public safety in NCUA facilities, to prevent crime, and to assist law enforcement agencies in criminal prosecutions. To address internal personnel, suitability and security clearance issues, and potential insider threats. To address internal personnel, suitability and security clearance issues, and potential insider threats. To share with law enforcement agencies for internal and external investigations.

Sharing of the PII

The NCUA Office of Inspector General, Federal, state or local law enforcement agencies, and contractors who work on the system.

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

PII about the public, NCUA contractors or employees in monitored areas may include: photos, license plate numbers of such individual's cars in NCUA's parking garage(s) or near NCUA's buildings, identifying text written on recorded individuals' belongings that may enter NCUA's buildings or parking garages, and potentially the identity of an individual including name and picture of the individual.

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

Data is potentially collected about the general public in monitored areas, including passersbys on public streets near NCUA's buildings and potentially in NCUA's parking garage(s). The system may also potentially collect data about NCUA employees or contractors pertaining to: internal personnel incidents, and/or actions related to one's suitability/security clearance to continue working for NCUA.

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 view and use video images is limited to authorized OCSM personnel and Security Guards with a need to know to perform their official duties. All authorized users must complete training before being granted access to use the system. Users must comply with NCUA rules of behavior governing use of IT systems and complete mandatory NCUA privacy and security training. Authorized users of the PACS will be able to use the video in one of two ways: (1) by logging onto the SMS workstation or (2) by viewing displays that feed live video from nearby CCTV cameras. A unique username and password to access the system. The security command center which houses the system has limited access to authorized personnel only who use their security badge on the electronic badge reader outside the door to access the command center. Audit trails are conducted to monitor authorized users use of the system.

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 NCUA-1.

Availability of Privacy Notices

The SORN and PIA for the Physical Access Control System (PACS) 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 6/29/18.

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