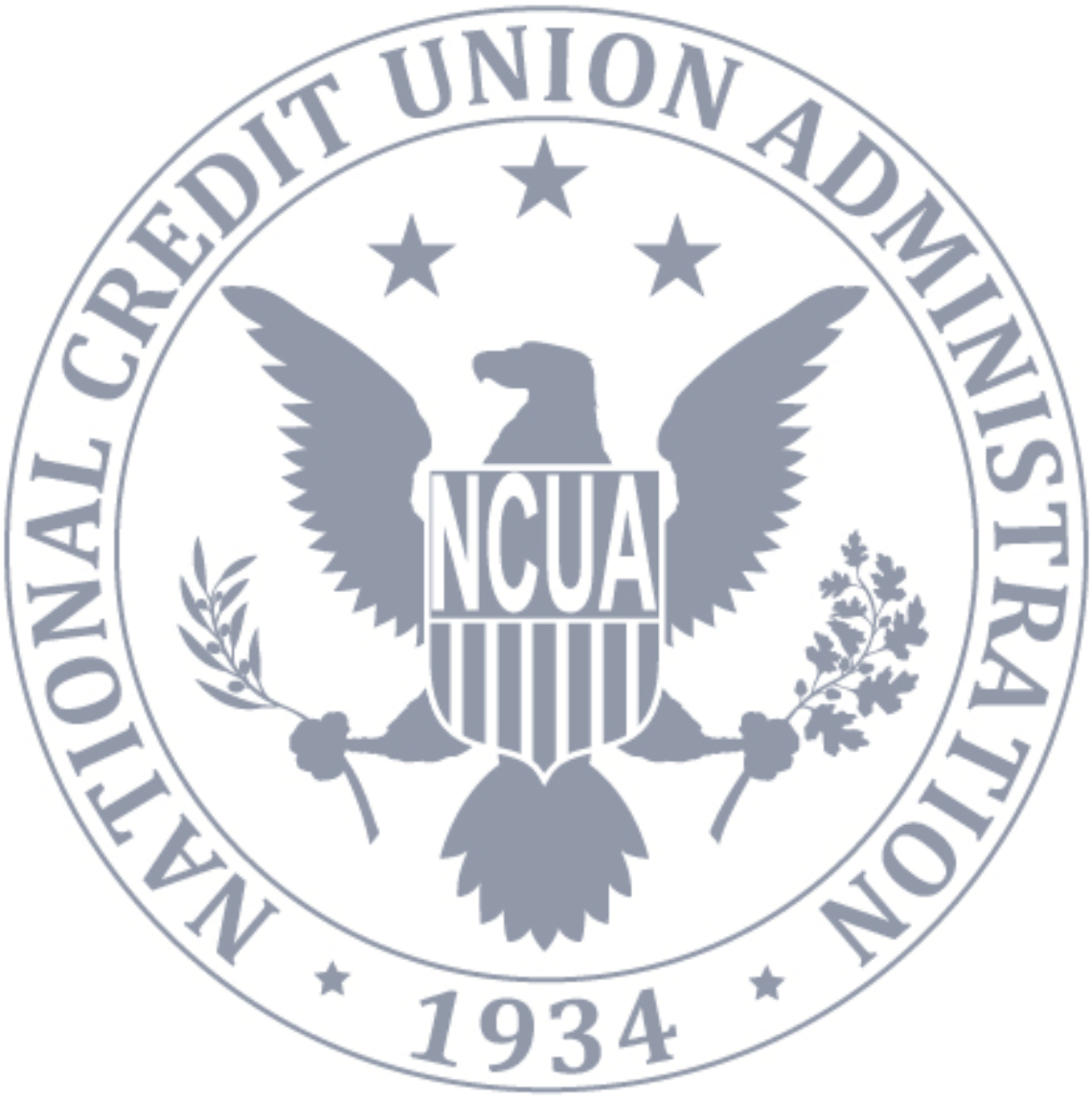
NCUA
National Credit Union Administration

Privacy Impact Assessment for GSA PIV USAccess

Fiscal Year 2018

[This page intentionally left blank]



PIA for GSA PIV USAccess • 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: GSA PIV USAccess

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

Executive Orders 10450, 10865, 12333, and 12356; 5 U.S.C. § 3301; 5 U.S.C. § 9101; 50 U.S.C. §§ 781-887; 5 C.F.R. Parts 732 and 736; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees

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

Records in the PIV IDMS are needed for credential management for enrolled individuals in the PIV program.

Intended Use of the PII Collected

The primary purposes of the system are: To ensure the safety and security of Federal facilities, systems, or information, and of facility occupants and users; to provide for interoperability and trust in allowing physical access to individuals entering Federal facilities; and to allow logical access to Federal information systems, networks, and resources on a government-wide basis.

Sharing of the PII

In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice (DOJ) when: (1) The agency or any component thereof; or (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (4) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are

both relevant and necessary to the litigation and the use of such records by DOJ and is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

b. To a court or adjudicative body in a proceeding when: (1) The agency or any component thereof; (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where the agency or the Department of Justice has agreed to represent the employee; or (4) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records and is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

c. Except as noted on Forms SF 85, SF 85–P, and SF 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

d. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

e. To the National Archives and Records Administration (NARA) or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

f. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract, service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a, the Federal Information Security Management Act (Pub. L. 107–296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration.

g. To a Federal agency, State, local, foreign, or tribal or other public authority,

on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

h. To the Office of Management and Budget (OMB) when necessary to the review of private relief legislation pursuant to OMB Circular No. A–19.

i. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended; the CIA Act of 1949, as amended; Executive Order 12333 or any successor order; and applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or Directives.

j. To designated agency personnel for controlled access to specific records for the purposes of performing authorized audit or authorized oversight and administrative functions. All access is controlled systematically through authentication using PIV credentials based on access and authorization rules for specific audit and administrative functions.

k. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Government Accountability Office (GAO), or other Federal agency in accordance with the agency's responsibility for evaluation of Federal personnel management.

l. To the Federal Bureau of Investigation for the FBI National Criminal History check.

m. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 types of PII collected in this system include:

- Full name;
- Social Security Number;
- Applicant ID number;
- Date of birth;
- Current address;
- Digital color photograph;
- Fingerprints;
- Biometric template (two fingerprints);
- Organization/office of assignment;
- Employee affiliation;
- Work email address;
- Work telephone number(s);
- Office address;
- Copies of identity source documents;
- Employee status;
- Military status;
- Foreign national status;
- Federal emergency response official status;
- Law enforcement official status;
- Results of background check;
- Government agency code; and
- PIV card issuance location.

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

Individuals consent to their personally identifiable information being stored in this system.

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

Federal Applicants, Contractors and Interns at NCUA Physical Security Central Office.

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

Consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107–296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services

Administration, the GSA HSPD–12 managed service office protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a ‘‘need to know’’ basis, utilization of PIV Card access, secure VPN for Web access, and locks on doors and approved storage containers. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All data is encrypted in transit.

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-17; GSA/GOVT-7.

Availability of Privacy Notices

The SORN and PIA for the GSA PIV USAccess 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 10/18/17.

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