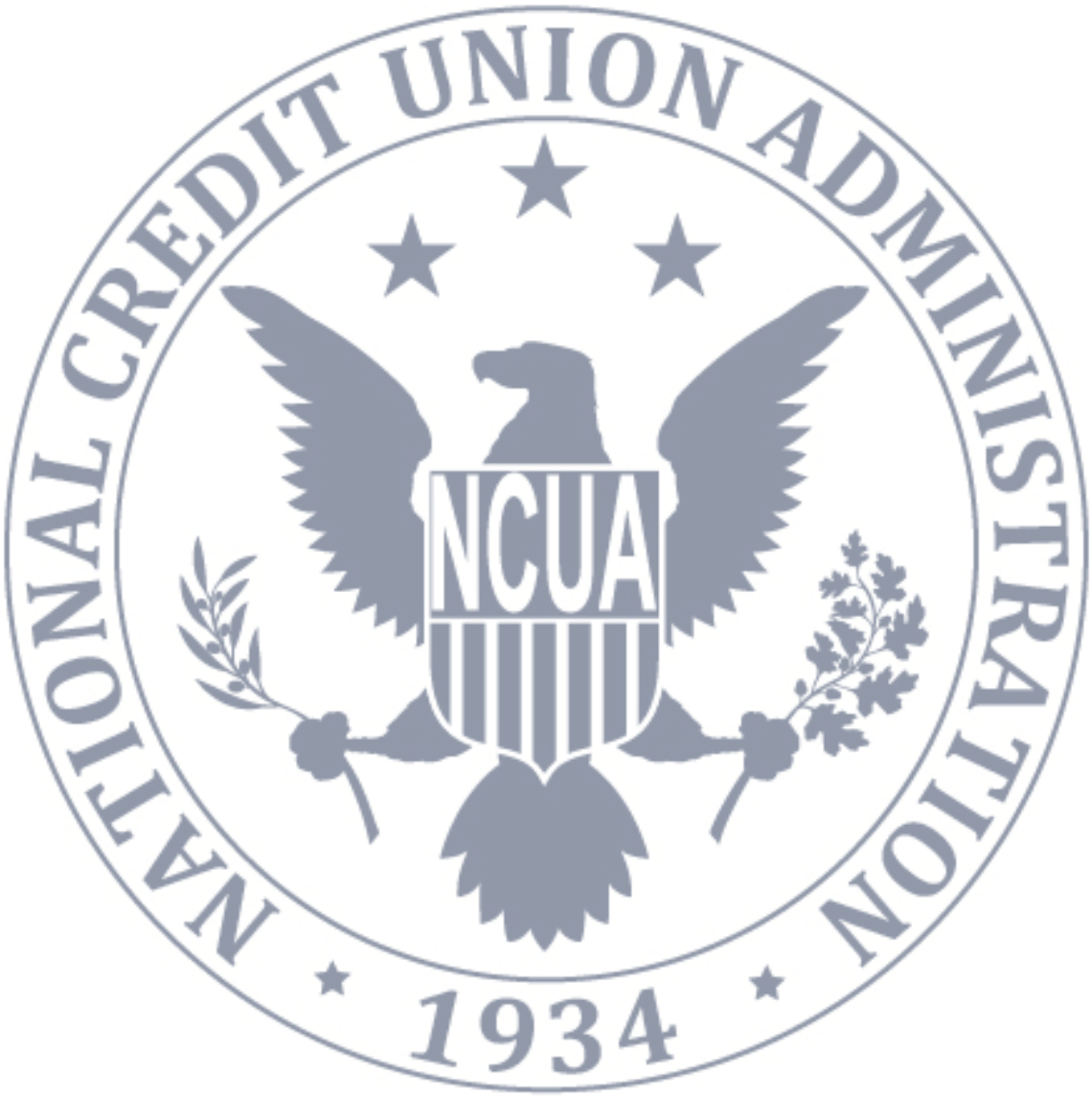
NCUA
National Credit Union Administration

Privacy Impact Assessment for ESS-MERIT

Fiscal Year 2019

[This page intentionally left blank]



PIA for ESS-MERIT • FY2019

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: ESS-MERIT

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).

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

ESS - MERIT will assist in accomplishing the NCUA's statutorily mandated examination and supervision activities, including the coordination and conduct of examinations, supervisory evaluations and analyses, enforcement actions and Federal court actions. NCUA may coordinate with other financial regulatory agencies on matters related to the safety and soundness of credit unions. The information collected in this system will also support the conduct of investigations or be used as evidence by the NCUA or other supervisory or law enforcement agencies. This may result in criminal referrals, referrals to Offices of Inspectors General, or the initiation of administrative or Federal court actions. This system will track and store examination and supervision documents created during the performance of the NCUA's statutory duties. The information will also be used for administrative purposes to ensure quality control, performance, and improving examination and supervision processes.

Intended Use of the PII Collected

NCUA intends to transform credit union examination and supervision processes and tools to enable proactive, risk-focused, data driven decisions and to enhance efficiency, security, and business agility.

As the primary tool for NCUA's examination and supervision responsibilities, ESS-MERIT will be used by the NCUA and state examiners to review and analyze data related to the operations of federally insured credit unions and some state-chartered, non-federally insured credit unions. ESS-MERIT is based on the Metricstream Governance, Risk, and Compliance (GRC) commercial-off-the-shelf (COTS) solution. The system will aggregate quarterly credit union reports that capture financial and operational data about credit unions, including information about credit union officials. The system will also facilitate the NCUA's review of individuals' credit union share and loan information.

Sharing of the PII

Access to ESS - MERIT is restricted to only authorized, named individuals with a need to know, least privileged access is enforced, and the flow of information is restricted (where appropriate). This will initially include NCUA staff, system integrator contractors (with signed Non-Disclosure Agreements), and representatives from North Carolina and Washington State Supervisory Authorities (SSAs) who are on our Integrated Project Teams (IPTs) who will have access only to data associated with credit unions in their states. After full system implementation, the remaining SSAs will have access only to data associated with credit unions in their states.

1. A financial institution affected by enforcement activities or reported criminal activities;
2. The Internal Revenue Service and appropriate State and local taxing authorities;
3. To another federal or state agency to: (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records;
4. To a grand jury pursuant either to a federal or state grand jury subpoena, or to a prosecution request that such record be released for the purpose of its introduction to a grand jury, where the subpoena or request has been specifically approved by a court;
5. To a court, magistrate, or administrative tribunal in the course of an administrative proceeding or judicial proceeding, including disclosures to opposing counsel or witnesses (including expert witnesses) in the course of

discovery or other pre-hearing exchanges of information, litigation, or settlement negotiations, where relevant or potentially relevant to a proceeding related to the NCUA's mission of providing a safe and sound credit union system.

6. To appropriate agencies, entities, and persons, including but not limited to potential expert witnesses, witnesses, or translators, in the course of supervision or enforcement related investigation;
7. To appropriate federal, state, local, foreign, tribal, or self-regulatory organizations or agencies responsible for investigating, prosecuting, enforcing, implementing, issuing, or carrying out a statute, rule, regulation, order, policy, or license if the information may be relevant to a potential violation of civil or criminal law, rule, regulation, order, policy, or license; and
8. To an entity or person that is the subject of supervision or enforcement activities including examinations, investigations, administrative proceedings, and litigation, and the attorney or non-attorney representative for that entity or person.

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

Records in the system may contain: (1) Contact information about credit union officials (such as members of the Board of Directors, Audit Committee Chair, Chief Executive Officer, Chief Compliance Officer, Internal Auditor, and Independent Auditor), such as name, address, phone number, and e-mail address; (2) Demographic and financial information about individual credit union members, such as name, address, Social Security number, account information, loan and share information, and publicly available information; (3) Information about NCUA employees assigned to credit union examination and supervision tasks, such as name, work phone number, work e-mail address, and other employment information; (4) User information, such as name, email

address, and role about other users of the system (such as contractors, credit union representatives, State Supervisory Authority staff, and Credit Union Service Organization representatives (CUSOs).

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

The information in the system about credit union officials and individual credit union members is generally provided by credit unions and CUSOs. NCUA employees and contractors, and State Supervisory Authorities may add additional information to the system as part of their assigned supervision and examination activities (including analytics/business intelligence activities). Some of the information may be from third parties with relevant information about covered persons or service providers, or existing databases maintained by other Federal and state regulatory associations, law enforcement agencies, and related entities. Whenever practicable, the NCUA collects information about an individual directly from that individual.

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

PII is stored on dedicated secure servers, approved by NCUA's Office of the Chief Information Officer (OCIO), within a FedRAMP-authorized commercial Cloud Service Provider's (CSP) Infrastructure as a Service (IaaS) hosting environment and accessed only by authorized personnel.

Access rights to the data are restricted based on job function and the principle of least privilege.

Granting access is based upon:

- A valid access authorization,
- Intended data and system use,
- Request approved by the system manager.

Data in transit and at rest is encrypted, data is hosted in a FedRAMP certified for Government use only environment, and is protected by several layers of firewalls, proxies, and network security appliances. Furthermore, the environment is monitored by

dedicated security applications and services put in place to detect and alert on unauthorized network traffic, unauthorized access, and violations of rules and regulations.

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-22.

Availability of Privacy Notices

The SORN and PIA for the ESS-MERIT 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 2/28/19.

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