NATIONAL CREDIT UNION ADMINISTRATION

Privacy Act of 1974: System of Records

AGENCY: National Credit Union Administration (NCUA).

ACTION: Notice of Altered Privacy Act System of Records.

SUMMARY: The Personnel Administrative Security System collects and maintains information on individuals requiring access to NCUA-controlled facilities and NCUA applicants, employees, and contractors requiring suitability, fitness, and/or national security determinations.

DATES: Submit comments on or before April 5, 2016. This action will be effective without further notice on April 12, 2016 unless comments are received that would result in a contrary determination.

ADDRESSES: You may submit comments by any of the following methods, but please send comments by one method only:

• Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

• NCUA Web site: http://www.ncua.gov/RegulationsOpinionsLaws/proposed_regs/proposed_regs.html. Follow the instructions for submitting comments.

• Email: Address to regcomments@ncua.gov. Include ‘‘[Your name]—Comments on NCUA PASS Registry SORN’’ in the email subject line.

• Fax: (703) 518–6319. Use the subject line described above for email.

• Mail: Address to Gerard Poliquin, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314–3428.

• Hand Delivery/Courier: Same as mail address.

FOR FURTHER INFORMATION CONTACT: Charles Burr, System Manager, Office of Continuity and Security Management, Kevin Johnson, Staff Attorney, or Linda Dent, Senior Agency Official for Privacy, Office of General Counsel, at the National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia, 22314, or telephone: (703) 518-6540.

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974 (5 U.S.C. 552a), as amended, NCUA is issuing public notice of its intent to modify the system of records previously maintained by the Office of Human Resources (OHR) and titled “Employee Suitability and Security Investigations Containing Adverse Information, NCUA.” The proposed modifications will: change the system manager from OHR to the Office of Continuity and Security Management (OCSM); rename the system to the “Personnel Access and Security System (PASS);” restate the routine uses of records. This action is necessary to meet the requirements of the Privacy Act that federal agencies publish in the **Federal Register** a notice of

the existence and character of records it maintains that are retrieved by an individual identifier (5 U.S.C. 552a(e)(4)).

SYSTEM NAME AND NUMBER: Personnel Access and Security System (PASS), NCUA-1

SYSTEM LOCATION: Office of Continuity and Security Management, National Credit Union Administration, 1775 Duke Street, Alexandria, VA. 22314-3428.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Government Organization and Employees (5 U.S.C. 301); 5 U.S.C. Chapter 73 (Suitability, Security, and Conduct); 5 U.S.C. 7531-33 (National Security); Federal Information Security Management Act of 2002 (44 U.S.C. 3541); E-Government Act of 2002 (44 U.S.C. 101); Paperwork Reduction Act of 1995 (44 U.S.C. 3501); Executive Order 10450 (Security requirements for government employment); Executive Order 13526 and its predecessor orders (National Security Information); Executive Order 12968 (Access to Classified Information); Executive Order 13857 (Security of Classified Networks and Information); Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004); 12 U.S.C § 1785 and NCUA Rules and Regulations 701.14; Section 212 of the Federal Credit Union Act (12 U.S.C § 1790a).

PURPOSE(S): The collected information enables NCUA OCSM to identify and review allegations of misconduct or negligence in employment and other security information relevant to making HSPD-12 PIV card issuance determinations, and personnel suitability, fitness, and/or national security determinations. It also improves the handling of sensitive personal information and facilitates NCUA's ability to identify potential insider threats or potential systemic security concerns.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The system will collect and maintain information on individuals who require short- or long-term access as required by their position to NCUA-controlled facilities and information technology systems, including NCUA employees, appointees, interns, contractors, students, volunteers, and other non-federal employees either presently or formerly in any of these positions; applicants for NCUA employment or for work on NCUA contracts; applicants, appointees, employees, interns or contractors for whom an Office of Personnel Management (OPM) suitability, fitness or national security clearance investigation has been initiated and/or conducted; officials from troubled or newly chartered credit unions; visitors to NCUA facilities and their security clearance information; foreign national visitors.

CATEGORIES OF RECORDS IN THE SYSTEM: Incident and investigative material relating to any category of individual described above, including case files containing information such as full name, date of birth, gender, photograph, social security number, place of birth, citizenship; work and home telephone numbers and addresses; identification documentation (such as passports, work visas, driver's licenses); security screening information (such as resume, employer address, applications for employment, fingerprints, credit checks); legal case pleadings and files; employment information (NCUA employment status, former employment letters of reference, former employment letters of termination or resignation); information obtained during security inquires (such as letters of inquiry; other agency database

checks and reports; suspicious activity reports and notifications from other agencies and employees; network audit records, email, chat conversations, text messages sent using NCUA devices; social media account findings for individuals undergoing security investigations); self-reported security-related information (such as foreign travel notifications, changes in financial status, changes in marital status, arrests); security violation files; security evaluations and clearances; NCUA security screening status (permanent or provisional); personnel identity verification (PIV) information (such as card status, PIV card number, PIN number).

For visitors, information collected can include names, date of birth, citizenship, identification type, temporary pass number, host name, office symbol, room number, telephone number.

RECORD SOURCE CATEGORIES: Information is provided by the individual to whom the record pertains; references supplied by the individual such as current and/or former employers and associates; public records such as court documents, news media, social media and other publications; intra-agency records; and investigative and other record material compiled in the course of investigation or furnished by other government agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: NCUA OCSM uses these records to document the outcome of adjudicative determinations for the issuance of the HSPD-12 PIV card or the local agency access badge, and to document the outcome of adjudicative determinations for suitability, fitness, and/or national security clearances. Contact information is used for communication and authentication purposes. In addition with those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of records in this system may be disclosed to authorized federal or state entities as it is determined to be relevant and necessary.

POLICIES AND PRACTICE FOR STORAGE OF RECORDS: Records are stored electronically and physically.

POLICIES AND PRACTICE FOR RETRIEVABILITY OF RECORDS: Records are retrieved by individual identifiers such as name, social security number, or an individual identifier with non-individually identifiable information.

POLICIES AND PRACTICE FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained until they become inactive. Records become inactive when they are no longer useful for their collected purpose. Records are disposed in accordance with NCUA record retention schedules and consistent with destruction methods appropriate to the type of information.

PHYSICAL, PROCEDURAL, AND ADMINISTRATIVE SAFEGUARDS: Information in the system is safeguarded in accordance with the applicable laws, rules and policies governing the operation of federal information systems. Access to privacy-related information within the system is password protected and restricted to authorized personnel. Physical records in paper format are safeguarded in accordance with the applicable laws, rules and policies governing

privacy-related information. All records in paper format are stored under the requisite double-lock. Access to privacy-related information in paper format is restricted to authorized personnel.

SYSTEM MANAGER(S): Deputy Director, Office of Continuity and Security Management, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314-3428.

RECORD ACCESS PROCEDURES: Upon verification that an individual has a record in the system, as determined by the notification procedure below, the system manager will provide the procedure for gaining access to available records.

CONTESTING RECORD PROCEDURES: Requests to amend or correct a record should be submitted in writing to the system manager listed above in accordance with NCUA regulations at 12 CFR Part 792, Subpart E. Requesters must reasonably identify the record, specify the information being contested, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete.

NOTIFICATION PROCEDURE: An individual can determine if this system contains a record pertaining to the individual by addressing a request in writing to the system manager listed above in accordance with NCUA regulations at 12 CFR Part 792, Subpart E. The individual must provide his/her full name and identify the date he/she was associated with NCUA as well as contact information for a response. If there is no record on the individual, the individual will be so advised.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: In addition to any exemption to which this system is subject by Notices published by or regulations promulgated by OPM or the Director of National Intelligence, the system is subject to a specific exemption pursuant to 5 U.S.C. 552a (k)(5) to the extent that disclosures would reveal a source who furnished information under an express promise of confidentiality, or prior to September 27, 1975, under an express or implied promise of confidentiality.

By the National Credit Union Administration on March 3, 2016.

Gerard Poliquin,

Secretary of the Board.

[FR Doc. 2016-05313 Filed: 3/9/2016 8:45 am; Publication Date: 3/10/2016]