NATIONAL

Privacy Act of 1974; System of Records

AGENCY: National Credit Union Administration (NCUA).

ACTION: Notice of new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the National Credit Union Administration (NCUA) gives notice of a new proposed Privacy Act system of records. The new proposed system is Ensuring Workplace Health and Safety in Response to a Public Health Emergency, NCUA-24. This system will maintain information collected in response to a public health emergency, such as a pandemic or epidemic, from NCUA personnel, including political appointees, employees, contractors, detailees, consultants, interns, volunteers, and applicants for Federal employment. This system will store information pertaining to individuals in the performance of the NCUA's statutory duties.

DATES: This new system of record is applicable on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The routine uses in this new system of record are applicable 30 days after publication, unless the NCUA makes changes based on comments received. Written comments should be submitted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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

- Federal eRulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: (703) 518–6319. Include "[Your Name]—Comments on New System of Records, NCUA-24" in the transmittal.

• Mail: Address to Melane Conyers-Ausbrooks, 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: Linda Dent, Senior Agency Official for Privacy via email at privacy@NCUA.gov or at 703-518-6540.

SUPPLEMENTARY INFORMATION: Pursuant to the Privacy Act, 5 U.S.C. 552a, the NCUA is establishing a new system of records, NCUA-24, Ensuring Workplace Health and Safety in Response to a Public Health Emergency. The NCUA is committed to providing all NCUA personnel with a safe and healthy work environment. When Federal, state, or local authorities declare a public health emergency, and only as necessary to protect the health and safety of its workforce and the public the NCUA may develop and institute additional safety measures to protect the workforce and those individuals entering NCUA facilities. These measures may include instituting activities such as: (1) requiring NCUA personnel (including applicants for Federal employment) to provide information and/or submit to a medical screening before being allowed access to an NCUA facility, and (2) contact tracing. NCUA personnel may also need to provide information before being authorized for work-related travel.

In certain instances, depending on the type of record collected and maintained, for Federal employees, this information will also be maintained and covered by Office of Personnel Management/Government-10 Employee Medical File System Records (75 FR 35099, June 21, 2010). However, any collection and use of records covered by this system of records notice (SORN) is only permitted during times of a declared public health emergency or when the circumstances require the NCUA to collect and maintain such information on the various categories of individuals described below. The NCUA will collect and maintain information in

accordance with the Americans with Disabilities Act of 1990 and regulations and guidance published by the U.S. Occupational Safety and Health Administration, the U.S. Equal Employment Opportunity Commission, and the U.S. Centers for Disease Control and Prevention.

This notice satisfies the Privacy Act requirement that an agency publish a system of records notice in the Federal Register when there is an addition to the agency's systems of records. NCUA-24 is published in full below. All of the NCUA's SORNs are available at www.ncua.gov.

By the National Credit Union Administration Board.

Melane Conyers-Ausbrooks,

Secretary of the Board.

SYSTEM NAME AND NUMBER: Ensuring Workplace Health and Safety in Response to a Public Health Emergency, NCUA-24.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at NCUA facilities in Alexandria, Virginia and regional offices. Original and duplicate systems may exist, in whole or in part, at secure sites and on secure servers maintained by third-party service providers for the NCUA.

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 12 U.S.C. 1751, et seq.; Americans with Disabilities Act, including 42 U.S.C. 12112(d)(3)(B), 29 CFR 1630.2(r), and 1630.14(b), (c), and (d)(4); Workforce safety Federal requirements, including the Occupational Safety and Health Act of 1970, 5 U.S.C. 7902; 29 U.S.C. Chapter 15 (e.g., 29 U.S.C. 668), 29 CFR part 1904, 29 CFR 1910.1020, and 29 CFR 1960.66; Executive Order 12196; Executive Order 14043.

PURPOSE(S) OF THE SYSTEM: The information in the system is collected to assist the NCUA with maintaining a safe and healthy workplace and respond to a public health emergency (as defined by the U.S. Department of Health and Human Services and declared by its Secretary), such as a pandemic or epidemic. These measures may include instituting activities such as: (1) requiring NCUA personnel (including applicants for Federal employment) to provide information and/or submit to a medical screening before being allowed access to an NCUA

facility, and (2) contact tracing. NCUA personnel may also need to provide information before being authorized to travel.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals covered by this system include NCUA personnel, such as, political appointees, employees, contractors, detailees, consultants, interns, volunteers, and applicants for Federal employment

CATEGORIES OF RECORDS IN THE SYSTEM:

Information may include:

- Name
- Contact information (e.g., email address, phone number)
- Employee ID number
- Recent travel history
- Whether the individual provides dependent care for an individual in a high-risk category
- Health information, including:
    - Body temperature,
    - Confirmation of pathogen or communicable disease test,
    - Test results,
    - Dates, symptoms, potential or actual exposure to a pathogen or communicable disease,
    - Immunization or vaccination information;
    - Information to support a reasonable accommodation (for example, a request for exemption from a vaccination requirement), and
    - Other medical history related to the treatment of a pathogen or communicable disease

- Contact tracing information, including:
    - Dates when the individual visited the NCUA facility or event, or worked on-site on behalf of the NCUA,
    - Locations that the individual visited within the facility (e.g., office and cubicle number),
    - Duration of time spent in the facility, and
    - Whether the individual may have potentially come into contact with a contagious person while visiting the facility.

RECORD SOURCE CATEGORIES: The information in this system is collected in part directly from the individual. Information is also collected from security systems monitoring access to NCUA facilities, such as video surveillance and turnstiles, human resources systems, emergency notification systems, and Federal, State, and local agencies assisting with the response to a public health emergency. Information may also be collected from property management companies responsible for managing office buildings that house NCUA facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the NCUA as a routine use as follows:

1. To appropriate Federal, State, local and foreign authorities responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information 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;

2. To an authorized appeal grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee. Further, a record from any system of records may be disclosed as a routine use to the Office of Personnel Management in accordance with the agency's responsibility for evaluation and oversight of Federal personnel management;
3. To a court, magistrate, or other administrative body in the course of presenting evidence, including disclosures to counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal proceedings, when the NCUA is a party to the proceeding or has a significant interest in the proceeding, to the extent that the information is determined to be relevant and necessary;
4. To contractors, experts, consultants, and the agents thereof, and others performing or working on a contract, service, cooperative agreement, or other assignment for the NCUA when necessary for the purpose of assisting the NCUA's response to a public health emergency;
5. To appropriate agencies, entities, and persons when (1) the NCUA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the NCUA 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 the NCUA 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 the NCUA's efforts to

respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

6. To another Federal agency or Federal entity, when the NCUA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach;
7. To a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of infectious disease; and
8. To members of Congress in response to requests made at the request of and on behalf of their constituents.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic records and backups are stored on secure servers, approved by the NCUA's Office of the Chief Information Officer (OCIO), within FedRAMP-authorized commercial Cloud Service Providers' (CSP) Software-as-a-Service solutions hosting environments and accessed only by authorized personnel. No paper files are maintained.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by any of the following: name, office, or e-mail address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained and disposed of in accordance with the General Records Retention Schedules issued by the National Archives and Records Administration (NARA) or an NCUA records disposition schedule approved by NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The NCUA and the Cloud Service Provider have implemented the appropriate administrative, technical, and physical controls in accordance with the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, S. 2521, and the NCUA's information security policies to protect the confidentiality, integrity, and availability of the information system and the information contained therein. Access is limited only to individuals authorized through NIST-compliant Identity, Credential, and Access Management policies and procedures. The records are maintained behind a layered defensive posture consistent with all applicable Federal laws and regulations, including Office of Management and Budget (OMB) Circular A-130 and National Institute of Standards and Technology (NIST) Special Publications 800-37.

RECORD ACCESS PROCEDURES: Individuals wishing access to their records should submit a written request to the Senior Agency Official for Privacy, NCUA, 1775 Duke Street, Alexandria, VA 22314, and provide the following information:

1. Full name.
2. Any available information regarding the type of record involved.
3. The address to which the record information should be sent.
4. You must sign your request.

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf. Individuals requesting access must also comply with the NCUA's Privacy Act regulations regarding verification of identity and access to records (12 CFR 792.55).

CONTESTING RECORD PROCEDURES: Individuals wishing to request an amendment to their records should submit a written request to the Senior Agency Official for Privacy, NCUA, 1775 Duke Street, Alexandria, VA 22314, and provide the following information:

1. Full name.
2. Any available information regarding the type of record involved.
3. A statement specifying the changes to be made in the records and the justification therefore.
4. The address to which the response should be sent.
5. You must sign your request.

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf.

NOTIFICATION PROCEDURES: Individuals wishing to learn whether this system of records contains information about them should submit a written request to the Senior Agency Official for Privacy, NCUA, 1775 Duke Street, Alexandria, VA 22314, and provide the following information:

1. Full name.
2. Any available information regarding the type of record involved.
3. The address to which the record information should be sent.
4. You must sign your request.

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf. Individuals requesting access must also comply with the NCUA's Privacy Act regulations regarding verification of identity and access to records (12 CFR 792.55).

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: This is a new system.

[FR Doc. 2021-24704 Filed: 11/10/2021 8:45 am; Publication Date: 11/12/2021]