

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper and electronic.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by Name, SSN and Property Address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

(1) Payments and Disbursements files. Temporary. Destroy 6 years after final payment or cancellations, but longer retention is authorized if required for business use.

(2) System development/ infrastructure project files. Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use.

(3) System general technology management records. Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

(4) System technical documents. Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.

(5) System access records. Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

(6) System backups and tape library records (Incremental backup files). Temporary. Destroy when second subsequent backup is verified as successful, or when no longer needed for system restoration, whichever is later.

(7) System backups and tape (full backup files). Temporary. Destroy when subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

(8) System backup on master files. Temporary. Destroy when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

(9) Premium Refund Application website search files. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

(10) Premium Refund Application Upload page files. Temporary. Destroy upon verification of successful creation of the final document or file, or when

no longer needed for business use, whichever is later.

(11) System input/output files. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

(12) Paper Records and related technical documentation. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Administrative Controls: Backups Secured Off-Site, Methods to Ensure Only Authorized Personnel Access to PII, Periodic Security Audits, and Regular Monitoring of User's Security Practices. *Technical Controls:* Encryption of Data at Rest, Firewall, Role-Based Access Controls, Virtual Private Network (VPN), Encryption of Data in Transit, Least Privilege Access, User Identification and Password, PIV Card, Intrusion Detection System (IDS).

Physical Safeguards: Combination locks, Key Cards, Security Guards, Identification badges, and all paper records that contain PII and sensitive information are locked in file rooms.

RECORD ACCESS PROCEDURES:

Individuals seeking notification of and access to their records in this system of records may submit a request in writing to the Department of Housing and Urban Development, Attn: FOIA Program Office, 451 7th Street SW, Suite 10139, Washington, DC 20410-0001. or by emailing foia@hud.gov. Individuals must furnish the following information for their records to be located:

1. Full name.
2. Signature.
3. The reason why the individual believes this system contains information about him/her.
4. The address to which the information should be sent.

CONTESTING RECORD PROCEDURES:

Same as the Notification Procedures above.

NOTIFICATION PROCEDURES:

Any person wanting to know whether this system of records contains information about him or her should contact the System Manager. Such person should provide his or her full name, position title and office location at the time the accommodation was requested, and a mailing address to which a response is to be sent.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

DSRS SORN: 81 FR 22293 (April 15, 2016)

DSRS SORN: 72 FR 40890 (July 25, 2007)

LaDonne White,

Chief Privacy Officer, Office of Administration.

[FR Doc. 2022-22103 Filed 10-11-22; 8:45 am]

BILLING CODE 4210-67-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-7062-N-17]

Privacy Act of 1974: System of Records

AGENCY: Office of Chief Human Capital Officer, HUD.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of Housing and Urban Development (HUD), the Office of Chief Human Capital Officer (OCHCO), proposes to modify the records titled *Personnel Security Integrated Tracking System (PerSIST)*. PerSIST is an enterprise personnel security case management system that automates activities associated with the tracking of personnel security investigations for HUD. The Department of Housing and Urban Development is issuing a public notice of its intent to modify the Personnel Security Integrated System for Tracking (PerSIST). This system of records is being modified to make clarifying notification in the supplementary information that the process is being partially automated, which will become effective immediately.

DATES: Comments will be accepted on or before November 14, 2022. This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number by one method:

Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions provided on that site to submit comments electronically.

Fax: 202-619-8365.

Email: www.privacy@hud.gov.

Mail: Attention: Privacy Office;

LaDonne White, Chief Privacy Officer; The Executive Secretariat; 451 Seventh Street SW, Room 10139; Washington, DC 20410-0001.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

LaDonne White, 451 Seventh Street SW, Room 10139; Washington, DC 20410-0001; telephone number 202-708-3054 (this is not a toll-free number). Individuals who are hearing- or speech-impaired can dial 7-1-1 to access the Telecommunications Relay Service (TRS), which permits users to make text-based calls, including Text Telephone (TTY) and Speech to Speech (STS) calls. Individuals who require an alternative aid or service to communicate effectively with HUD should email the point of contact listed above and provide a brief description of their preferred method of communication.

SUPPLEMENTARY INFORMATION: The Personnel Security Integrated Tracking System (PerSIST) system of records was most recently published in the **Federal Register** on May 11th, 2018 (83 FR 22094). The Department is hereby modifying that notice by updating the supplementary information. PerSIST was integrated with the Government Services Administration's (GSA) USAccess system to help facilitate the issuance of the commonly approved credential (HSPD-12 Credential), often referred to as the Privately Identifiable Verification Card (PIV), that supports activities like enrollment, personal data updates, fingerprinting, badge pickup, sponsorship, and PIV credential operations. PerSIST was also integrated with the Defense Counterintelligence and Security Agency's Electronic Delivery (DCSA) (eDelivery) system, which is an electronic assembly and delivery of investigative case materials to the requesting agency. These integrations partially, automates HUD's process to subsequently, increase the timeliness and efficiency of the investigative process.

SYSTEM NAME AND NUMBER:

Personnel Security Integrated System for Tracking HUD/OCHCO-02.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the following locations: U.S. Department of

Housing and Urban Development Headquarters location, Room 2135, 451 7th Street SW, Washington, DC 20410-0001.

SYSTEM MANAGER(S):

Director, Cyrus Walker, Personnel Security Division (PSD), Office of the Chief Human Capital Officer (OCHCO), 451 7th Street SW, U.S. Department of Housing and Urban Development; Washington, DC 20410-000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Relative to the purpose of your investigation, the U.S government is authorized to request this information under Executive Orders: 10865, 12333, 12356, and 13764. Sections 3301 and 9101, of title 5, U.S. Code; section 2165 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 21, 2004. Amending the civil service rules, Executive Order 13488, and Executive Order 13467, Privacy Act of 1974, 5 U.S.C. 552a.

PURPOSE OF THE SYSTEM:

The purpose of the system is to allow HUD to document and support decisions regarding the suitability, eligibility, and fitness for services of applicants for federal employment and contract positions to include students, interns, or volunteers eligible for logical and physical access to federally controlled facilities and information systems; eligible to hold sensitive positions (including but not limited to eligibility for access to classified information); fit to perform work for or on behalf of the Government as a contractor employee; qualified for Government service; qualified to perform contractual services for the Government; and loyal to the United States. Another purpose for this system is also to document such determinations, and to otherwise comply with mandates and Executive Orders. These records may also be used to locate individual for personnel research, as well as to document security violations, and supervisory actions taken. Additionally, these records may be used to help streamline the investigations and adjudications processes generally.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current HUD Employees, Applicants, Contractors, Students, Interns, and volunteers

CATEGORIES OF RECORDS IN THE SYSTEM:

Full Name, date of birth, birthplace, social security number, home address, phone numbers, employment history, contact information, citizenship, relatives, birth dates, birth place; criminal history, mental health history, history of drug use, financial information, fingerprints, report of investigation, results of suitability decisions, security clearance(s); date of issuance, request for appeal, witness statements, investigator's notes, tax returns, credit reports, security violations, circumstances of violation, and agency action taken.

RECORD SOURCE CATEGORIES IN THE SYSTEM:

Individuals, Defense Counterintelligence and Security Agency, Office of Personnel Management, GSA. OPM e-QIP
—General Services Administration (GSA) USAccess- Defense Counterintelligence Security Agency (DCSA) e-Delivery

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. To a congressional office from the record of an individual, in response to an inquiry from the congressional office made at the request of that individual.
2. To appropriate Federal, State, local, tribal, or governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where HUD determines that the information would assist in the enforcement of civil or criminal laws and when such records, either alone or in conjunction with other information, indicate a violation or potential violation of law.
- (3). To any component of the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when HUD determines that the use of such records is relevant and necessary to the litigation and when any of the following is a party to the litigation or have an interest in such litigation: (I) HUD, or any component thereof; or (II) any HUD employee in his or her official capacity; or (III) any HUD employee in his or her individual capacity where the Department of Justice or agency conducting the litigation has agreed to represent the employee; or (IV) the United States, or any agency thereof, where HUD determines that litigation is likely to affect HUD or any of its components.
4. (a) To appropriate agencies, entities, and persons when: (I) HUD

suspects or has confirmed that there has been a breach of the system of records; (II) HUD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HUD (including its information systems, programs, and operations), the Federal Government, or national security; and (III) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HUD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

5. (b) To another Federal agency or Federal entity, when HUD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (I) responding to a suspected or confirmed breach or (II) 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.

6. Accept as noted on Forms SF-85, 85P, and 86, when a record on its face, or in junction with other records, made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, 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.

7. To contractors, grantees, experts, consultants and their agents, or others performing or working under a contract, service, grant, or cooperative agreement with HUD or under contract to another agency when necessary to accomplish an agency function related to a system of records. Disclosure requirements are limited to only those data elements considered relevant to accomplishing an agency function.

8. 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, applicable national security directives, or classified implementing procedures with 54836 **Federal Register**/Vol. 71, No. 181/Tuesday, September 19, 2006/ Notices approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

9. To the Office of Personnel Management (OPM), the Merit Systems Protection Board (and its office of the Special Counsel), the Federal Labor Relations Authority (and its General Counsel), or the Equal Employment Opportunity Commission when requested in performance of their authorized duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper and electronic records.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by name and social security number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Destroy 3 years after employee separation from the agency or all appeals are concluded whichever is later, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

For Paper Records: Comprehensive paper records are kept in locked metal file cabinets in locked rooms in HUD Headquarters, in the Personnel Security Division which is the office responsible for suitability determinations. Access to the records is limited to those employees who have a need for them in the performance of their official duties.

For Electronic Records: Comprehensive electronic records are kept in the Personnel Security Division. Access to the records is restricted to those who have specific roles in the Personal Security Division and require access to background investigative data to perform their duties; and who have been given a password or two (2) factor authentication to access applicable files within the system including background investigative data. An electronic audit trail is maintained within the system and reviewed periodically to identify and track authorized/unauthorized access.

For Electronic Records (cloud based): Comprehensive electronic records are secured and maintained on a cloud-based software server and operating system that resides in Federal Risk and Authorization Management Program (FedRAMP) and Federal Information Security Management Act (FISMA) Moderate dedicated hosting environment. All data located in the cloud-based server is firewalled and encrypted at rest and in transit. The security mechanisms for handing data at

rest and in transit are in accordance with HUD encryption standards.

RECORD ACCESS PROCEDURES:

Individuals seeking notification of and access to their records in this system of records may submit a request in writing to the Department of Housing and Urban Development, Attn: FOIA Program Office, 451 7th Street SW, Suite 10139, Washington, DC 20410-0001 or by emailing foia@hud.gov. Individuals must furnish the following information for their records to be located:

1. Full name.
2. Signature.
3. The reason why the individual believes this system contains information about him/her.
4. The address to which the information should be sent.

CONTESTING RECORD PROCEDURES:

Same as the Notification Procedures below.

NOTIFICATION PROCEDURES:

Any person wanting to know whether this system of records contains information about him or her should contact the System Manager. Such person should provide his or her full name, position title and office location at the time the accommodation was requested, and a mailing address to which a response is to be sent.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Persist system published in the **Federal Register** dated May 11, 2018 (83 FR 22094).

LaDonne White,
Chief Privacy Officer, Office of Administration.

[FR Doc. 2022-22104 Filed 10-11-22; 8:45 am]

BILLING CODE 4210-67-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-6357-N-01]

Notice of HUD-Held Multifamily and Healthcare Loan Sale (MHLS 2023-1)

AGENCY: Office of the Assistant Secretary for Housing—Federal Housing Commissioner, HUD.

ACTION: Notice of sale of one multifamily and 15 healthcare mortgage loans.

SUMMARY: This notice announces HUD's intention to sell one unsubsidized multifamily and fifteen unsubsidized healthcare mortgage loans, without