

Collection of Information

Title: Application for Surplus Federal Real Property Public Benefit Conveyance and BRAC Program for Emergency Management Use.

Type of Information Collection: Extension of a currently approved information collection.

OMB Number: 1660–0080.

FEMA Forms: FEMA Form FF–119–FY–22–133, Application for Surplus Federal Real Property Public Benefit Conveyance.

Abstract: Use of the Application for Surplus Federal Real Property Public Benefit Conveyance and Base Realignment and Closure (BRAC) Program for Emergency Management Use is necessary to implement the processes and procedures for the successful, lawful, and expeditious conveyance of real property from the Federal government to public entities such as State, local, county, city, town, or other like government bodies, as it relates to emergency management response purposes, including fire and rescue services. Utilization of this application will ensure that properties will be fully positioned for use at their highest and best potentials as required by GSA and DOD/DOW regulations, public law, Executive Orders, and the CFR.

Affected Public: State, Local or Tribal Government.

Estimated Number of Respondents: 15.

Estimated Number of Responses: 15.

Estimated Total Annual Burden Hours: 68.

Estimated Total Annual Respondent Cost: \$4,436.

Estimated Respondents' Operation and Maintenance Costs: \$0.

Estimated Respondents' Capital and Start-Up Costs: \$0.

Estimated Total Annual Cost to the Federal Government: \$4,003.

Comments

Comments may be submitted as indicated in the **ADDRESSES** caption above. Comments are solicited to (a) evaluate whether the proposed data collection is necessary for the proper performance of the Agency, including whether the information shall have practical utility; (b) evaluate the accuracy of the Agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) enhance the quality, utility, and clarity of the information to be collected; and (d) minimize the burden of the collection of information on those who are to respond, including through

the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

Russell R. Bard,

Information Management Senior Director, Office of the Chief Administrative Officer, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.

[FR Doc. 2026–15333 Filed 7–29–26; 8:45 am]

BILLING CODE 9111–19–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7106–N–34]

Privacy Act of 1974; System of Records

AGENCY: Office of Chief Information Security Officer, HUD.

ACTION: Notice of a new system of record.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of Housing and Urban Development (HUD), Office of Chief Information Security Officer (OCISO) is issuing public notice of its intent to create a new system of record titled Enterprise Identity and Credential Access Management (EICAM). The purpose of EICAM is to standardize user access controls, which provides support for users through self-service functions, and ensure only approved users may access HUD systems and data across the HUD enterprise. EICAM more efficiently reinforces the rules and controls governing the collection, maintenance, use, and sharing of information.

DATES: Comments will be accepted on or before August 31, 2026. 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 the docket number or by one of the following methods:

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

Fax: 202–619–8365.

Email: privacy@hud.gov.

Mail: Attention: Privacy Office; Kimberly Morton, Acting Chief Privacy Officer; Office of the Executive Secretariat; 451 7th 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:

Kimberly Morton, Acting Chief Privacy Officer; 451 7th Street SW, Room 10139; Washington, DC 20410–0001; telephone number (804) 822–4801 (this is not a toll-free number). HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit <https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs>.

SUPPLEMENTARY INFORMATION: HUD is establishing the Enterprise Identity Credential Access Management (EICAM) records as a HUD-wide Privacy Act system of records. EICAM is a Framework developed by the Chief Information Officer/Chief Information Security Officer Program Office. The EICAM Framework is the centralized department-wide infrastructure designed to manage the full lifecycle of digital identities, credentials, and access permissions. Its foundational role within HUD is to enforce a Zero Trust Architecture (ZTA) in alignment with Executive Order 14028 and OMB M–22–09, while meeting the federal identity consolidation frameworks established under OMB M–19–17. EICAM ensures that the right individual has the right level of access to the right HUD resources, at the right time, and for the right reason. In accordance with HUD's WEB Access Security Subsystem (WASS) modernization directives, EICAM unifies fragmented legacy identities.

A key component of the EICAM framework is the Web Access Security Subsystem (WASS). Currently, WASS facilitates secure access to HUD systems by managing authentication for both internal and external users through a combination of identity verification services, including multi-factor authentication.

EICAM manages user identities and access across the enterprise using Okta as the primary directory for HUD-defined PII, including usernames, contact details, and dates of birth. By utilizing unique identifiers, EICAM eliminates the need to store Social

Security Numbers. Identity proofing is supported by Socure, a Software-as-a-Service (SaaS) platform that provides identity verification and fraud prevention solutions, with Okta profiles updated upon successful verification. Internal identity data is maintained within the HUD Active Directory, while sensitive financial and application-specific records remain in dedicated HUD databases. Furthermore, the system leverages the Federal Housing Administration Connection (FHAC) Authority to Operate (ATO) for external data collection, explicitly ensuring that Social Security Administration (SSA)-provided PII which is not shared with EICAM. As HUD evolves, these records will be increasingly consolidated into the Okta Universal Directory, which will serve as the centralized, cloud-based source of truth for all user and device identities.

This system of records covers the agency's maintenance of records about individual users of the HUD network and information systems, to create a secure and trusted environment where users can access authorized resources. HUD uses a Federal Risk and Authorization Management Program (FedRAMP) authorized Identity-as-a-Service (IDaaS) cloud platform to secure and validate internal and external user identities. This platform integrates with device-level signals alongside identity information for resource access with flexible adaptive MFA integrations at the application layer. The platform supports the hybrid cloud model allowing authentication of on-premises resources and has over 7,500 integrations available to other capabilities. The platform has implemented MFA for access to HUD On-Premises or Cloud applications through the integration of Personal Identity Verification (PIV) smartcards for HUD internal users or a verification and a One-Time Passcode (OTP) authenticator for HUD internal or external users. Additionally, the platform supports Single Sign On (SSO). There are significant advantages in providing EICAM services at the enterprise level, including efficiencies in consolidating network services; improved security; cost savings; and enabling the creation of digital identities for a single individual for use across the enterprise.

SYSTEM NAME AND NUMBER:

Enterprise Identity, Credential, and Access Management (EICAM), HUD/OCIO-07.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The system files are maintained in the Okta GovCloud, the identity authentication cloud service environment located within the Amazon Web Services (AWS) GovCloud; Cloud infrastructure and perimeter security service routing are provided by third-party vendor Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107. Records are transiently processed, routed, and cached across Cloudflare's geographically decentralized network of authorized FedRAMP Moderate points of presence. A comprehensive listing of domestic physical data center locations utilized within the FedRAMP boundary is maintained by the Cloudflare FedRAMP program management team.

SYSTEM MANAGER(S):

Tarrazzia Martin, Zero Trust Architecture (ZTA) EICAM Program Manager, 451 7th Street SW, Washington, DC 20410, telephone number (202) 402-3410.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 *et seq.*; Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.*; 6 U.S.C. 1523(b)(1); 42 U.S.C. 3535(d); Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 2015); and OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019); Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021); and OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022).

PURPOSES OF THE SYSTEM:

The principal purpose of the EICAM system is to capture and maintain a record of names, digital signatures, approved access, and other identifiers from authoritative sources to provide and maintain a record of access management to agency systems and resources, to include Financial Management and Reporting Records and Information Systems Security records.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have been issued credentials for access to HUD data, systems, or facilities which may include HUD employees; former employees and retirees; contractors and grantees; state and local government partners; public

housing authorities; private sector partners; lenders participating in HUD-insured loan programs; tenants and program beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records maintained within this system encompass a variety of data points necessary for identity management and secure operations. Personal identifying information includes basic biographical details such as full names, unique user identifiers (such as CID numbers for contractors and HUD numbers for employees), dates and places of birth, gender, citizenship, and mother's middle or maiden name. Additionally, the system may store contact and credentialing data, including email addresses, personal and work phone numbers, emergency contact information, photographs, race and ethnic origin, and details from government-issued identification such as driver's licenses or passports.

Employment and professional information are also collected to manage system roles and permissions. This includes the individual's employer and work address, employment status, duty position, grade, series, and office affiliation. To ensure users are qualified for specific access levels, the system tracks certifications, training completion records, and the specific access rights provisioned across various HUD applications.

To maintain a secure environment, the system processes authentication, device, and fraud prevention data. This involves identity verification materials, such as photographs of government IDs, self-photographs, and MFA elements like one-time passcodes and security questions. HUD also monitors technical metadata, including IP addresses, browser types, and usage patterns, alongside risk scores and transaction details provided by third-party identity proofing and fraud prevention services. Finally, system access and audit information—including login attempts, system usage logs, and data access records—is maintained to ensure accountability and monitor for unauthorized activity.

RECORD SOURCE CATEGORIES:

Records are obtained from the Web Access Security System (WASS), HUD Active Directory, the HUD Integrated Human Resources and Training System (HIHRTS), the HUD Intranet/LDAP services, the Okta Identity-as-a-Service (IDaaS) cloud platform, FHAC, and Socure.

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

(1) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

(2) To appropriate Federal, State, local, tribal, or other 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: (1) HUD, or any component thereof; or (2) any HUD employee in his or her official capacity; or (3) 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 (4) the United States, or any agency thereof, where HUD determines that litigation is likely to affect HUD or any of its components.

(4) To a court, magistrate, administrative tribunal, or arbitrator in the course of presenting evidence, including disclosures to opposing counsel or witnesses or jurors in the course of civil discovery, litigation, mediation, or settlement negotiations, or in connection with criminal law proceedings; when HUD determines that 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: (1) HUD, or any component thereof; or (2) any HUD employee in his or her official capacity; or (3) any HUD employee in his or her individual capacity where HUD has agreed to represent the employee; or (4) the United States, or any agency thereof, where HUD determines that litigation is likely to affect HUD or any of its components.

(5) To the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(6) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(7) To appropriate agencies, entities, and persons when (1) HUD suspects or confirms a breach of the system of records; (2) HUD determines 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 (3) 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.

(8) 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 (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.

(9) To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended.

(10) To Federal agencies and third parties for identity proofing, verification services, and fraud prevention services as necessary to detect fraud, investigate, and authenticate users for access to HUD systems or applications, including to provide redress to users.

(11) To third-party entities to conduct studies for secure sign-in service enhancements and demographic studies for equitable performance of new technologies and to guide service improvement.

(12) To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies,

procedures and compliance with the Freedom of Information Act (FOIA), and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic format only. Electronic records are stored within HUD-authorized systems, utilizing industry-standard encryption and restricted-access directories to ensure data security.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved from Okta by Username, Name, Address, Email, Date of Birth, and Phone Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS

Records are managed in accordance with the General Records Schedule (GRS) 5.5, System Access Records, items 010, which cover Mail, Printing, and Telecommunication Service Management Records. These records are temporary and are destroyed when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

HUD protects the records within this system through a multi-layered security strategy that adheres to all applicable federal rules, policies, and procedures. Administrative safeguards ensure that only authorized personnel interact with the data; this includes mandatory privacy and information assurance training for all users, strict adherence to "need-to-know" access principles, and continuous risk monitoring. To maintain system integrity, HUD conducts regular security assessments and maintains comprehensive incident response procedures to address potential breaches.

Technical safeguards utilize industry-standard encryption to secure data both at rest and during transit. Access is strictly controlled through Multi-Factor Authentication (MFA), including the use of Personal Identity Verification (PIV) cards and complex password requirements. The system is further protected by robust account management, regular vulnerability patching, and intrusion detection systems. Additionally, HUD employs data masking and anonymization techniques to shield sensitive information and maintains detailed logs to monitor all system activities.

Physical safeguards protect the hardware and facilities housing the system. Access to these data centers is restricted by multifactor physical controls, video surveillance, and alarm systems. All visitors are subject to logging and escort procedures to ensure facility security. Finally, HUD utilizes environmental controls—such as fire suppression and temperature regulation—to protect equipment, alongside secure disposal methods for electronic media to prevent any unauthorized recovery of data.

RECORD ACCESS PROCEDURES:

Individuals requesting records of themselves should address written inquiries to the Department of Housing and Urban Development 451 7th Street SW Washington, DC 20410–0001. For verification, individuals should provide their full name, current address, and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made under 24 CFR 16.4.

CONTESTING RECORD PROCEDURES:

The HUD rule for contesting the content of any record pertaining to the individual by the individual concerned is published in 24 CFR 16.8 or may be obtained from the system manager.

NOTIFICATION PROCEDURES:

Individuals requesting notification of records of themselves should address written inquiries to the Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410–0001. For verification purposes, individuals should provide their full name, office or organization where assigned, if applicable, and current address and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made under 24 CFR 16.4.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Kimberly Morton,

Acting Chief Privacy Officer, Office of Administration.

[FR Doc. 2026–15428 Filed 7–29–26; 8:45 am]

BILLING CODE 4210–67–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7106–N–33]

Privacy Act of 1974; System of Records

AGENCY: Office of Chief Human Capital Officer (OCHCO), HUD.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of Housing and Urban Development (HUD), Office of the Chief Human Capital Officer (OCHCO) is issuing a public notice of its intent to establish a new Privacy Act System of Records Notice (SORN) titled, “Human Resources Service Delivery (HRSD)”. The system aims to streamline the federal hiring process and enhance data accuracy by automating information exchange between HUD’s integrated core platforms and USA Staffing’s integrated Data Application Programming Interfaces (API) like, New Hire Interconnection (NHI), and Request Processing Interconnection (RPI). These interfaces enhance HRSD’s integration and data utilization across HUD systems and helps streamlines onboarding, transferring new hire data seamlessly, and helps to manage of the entire hiring process from requisition to onboarding, with bi-directional data exchange. The information maintained within Human Resources Service Delivery is sourced through the Office of Personnel Management’s (OPM), USA Staffing.

DATES: Comments will be accepted on or before August 31, 2026. 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 or by one of the following methods:

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

Fax: 202–619–8365.

Email: privacy@hud.gov.

Mail: Attention: The Privacy Office; Kimberly Morton, Acting Chief Privacy Officer; The Executive Secretariat; 451 7th 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:

Kimberly Morton, Acting Chief Privacy Officer; 451 7th Street SW, Room 10139; Washington, DC 20410–0001; telephone number (804) 822–4801 (this is not a toll-free number). HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit <https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs>.

SUPPLEMENTARY INFORMATION: HUD Office of the Chief Human Capital Officer (OCHCO) will implement the Human Resources Service Delivery (HRSD) system with case management capabilities to track and manage all HR service requests from initial submission to resolution. HUD seeks to reduce costs, streamline processes, and reduce the need for manual intervention. HRSD is designed to improve employee productivity through capabilities such as: Onboarding, Shared Certificates, Employee and Labor Relations, and Performance Recognition Management Solutions. HRSD collects and processes information through a structured data interconnection that streamlines employees onboarding and supports standardized workflows, reduces administrative burden, and enables faster resolution of requests, allowing employees to effectively locate information and answers independently. Additionally, HRSD will enhance the overall employee experience by providing a unified self-service portal to access HR services and HR information within the HUD cloud architecture through ServiceNow, a Government Community Cloud (GCC) offering that delivers the Now Platform and complies with stringent cloud security and privacy compliance requirements. The following capabilities address human resources requirements:

- *Classification:* Creating, managing, and tracking job requisitions and associated documentation.
- *Recruiting:* Managing recruitment actions, tracking job requisitions and maintaining related documentation.
- *Workforce Planning:* Supporting succession planning and future organizational structures to align current and future talent needs.
- *Onboarding:* Integrating new hires into existing human capital management (HCM) systems, including pay, position, and organizational data.