



DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-5763-N-09]

Implementation of the Privacy Act of 1974, as amended;

New System of Records Notice, Digital Identity Access Management System

AGENCY: Office of the Chief Information Officer.

ACTION: Notification.

SUMMARY: Pursuant to the Privacy Act of 1974 (U.S.C. 552a (e)(4)), as amended, and Office of Management and Budget (OMB), Circular No. A-130, notice is hereby given that the Department of Housing and Urban Development (HUD), Office of the Chief Information Officer (OCIO) proposes to establish a new system of records, the Digital Identity Access Management System (DIAMS). DIAMS will manage core digital identification, credential and access management (ICAM) data elements. The system will support the administration of the Homeland Security Presidential Directive 12 (HSPD-12) program that directs the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems. This system will enhance security, increase efficiency, protect personal privacy, and provide synchronization of core identity management data for Departmental systems.

DATES: **EFFECTIVE DATE:** This action shall be effective without further notice on **[Insert 30 days, after publication of this notice in the Federal Register]** unless comments are received that would result in a contrary determination.

[COMMENTS DUE DATE: [Insert 30 days after publication of this notice in the Federal Register].

ADDRESSES: Interested persons are invited to submit comments regarding this notice to the Rules Docket Clerk, Office of the General Counsel, Department of Housing and Urban Development, 451 Seventh Street, SW, Room 10276, Washington, DC 20410-0500.

Communication should refer to the above docket number and title. A copy of each communication submitted will be available for public inspection and copying between 8:00 am and 5:00 pm weekdays at the above address.

FOR FURTHER INFORMATION CONTACT: Donna Robinson-Staton, Chief Privacy Officer, 451 Seventh Street, SW, Washington, DC 20410 (Attention: Capitol View Building, 4th Floor), telephone number: (202) 402-8073. [The above telephone number is not a toll free number.] A telecommunications device for hearing- and speech-impaired persons (TTY) is available by calling the Federal Information Relay Service's toll-free telephone number (800) 877-8339.

SUPPLEMENTARY INFORMATION: This system of records is maintained by HUD's Office of the Chief Information Officer, and includes users of HUD's information technology personally identifiable information that is retrieved by a name or unique identifier. The new system encompasses programs and services of the Department's data collection and management practices. Publication of this notice allows HUD to satisfy its reporting requirement and keep an up-to-date accounting of its system of records publication. The new system proposal will incorporate Federal privacy requirements and HUD policy requirements. The Privacy Act provides certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies to protect records contained in an agency system of records from unauthorized disclosure, by ensuring that information is current and collected only for its intended use, and by

providing adequate safeguards to prevent misuse of such information. Additionally, this notice demonstrates the Department's focus on industry best practices in protecting the personal privacy of the individuals covered by each system notification. This notice states the name and location of the record system, the authority for and manner of its operations, the categories of individuals that it covers, the type of records that it contains, the sources of the information for those records, the routine uses made of the records, and the type of exemption in place for the records. In addition, this notice includes the business address of the HUD officials who will inform interested persons of the procedures whereby they may gain access to and/or request amendments to records pertaining to them.

This publication does meet the threshold requirements for a new system and a report was submitted to the Office of Management and Budget (OMB), the Senate Committee on Homeland Security and Governmental Affairs, and the House Committee on Government Reform as instructed by Paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agencies Responsibilities for Maintaining Records About Individuals," July 25, 1994 (59 FR 37914).

AUTHORITY: 5 U.S.C. 552a; 88 Stat. 1896; 42 U.S.C. 3535(d).

September 19, 2014

Date

Rafael C. Diaz.
Chief Information Officer

[Docket No. FR-5763-N-09]

BILLING CODE: 4210-67

SYSTEM OF RECORDS NO.: OCIO/QN.01

SYSTEM NAME: Digital Identity Access Management System (DIAMS) - P281

SYSTEM LOCATION: U.S. Department of Housing and Urban Development, 451 Seventh Street, SW, Washington D.C. 20410; Hewlett-Packard Enterprise Services, Building 6000, 2020 Union Carbide Drive, South Charleston, WV 25303. Backup, recovery, and archived digital media is stored in secure facilities located with Iron Mountain, 1545 Hansford St., Charleston, WV 25311. The DIAMS is accessible from all systems connected to the HUD Intranet nationwide at HUD Field and Regional offices¹.

SECURITY CLASSIFICATION: Most identity records are not classified. However, in some cases, records of a few individuals, or portions of some records, may potentially be classified in the interest of national security.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The following are covered by the DIAMS: all users of HUD information technology systems including HUD employees and supporting contractors, students, interns, volunteers; affiliates of, and users from, State and local governments, non-profit organizations, academia, and third party business partners. The system does not apply to occasional visitors or short-term guests to whom HUD will issue temporary identification and credentials.

¹ <http://portal.hud.gov/hudportal/HUD?src=/localoffices>

CATEGORIES OF RECORDS IN THE SYSTEM: DIAMS will collect and store the First Name, Last Name, Address, City, State, Country, Date of Birth, Social Security Number, Agency Rank, Agency, US Citizen Status, User Principal Name (UPN), AD Identifier, Distinguished Name, Common Name, Display Name, User Password, Email Address and Unique User ID (e.g., H or C ID numbers).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The authority for maintenance of the system and authorizes the collection of information is the Federal Information Processing Standards, 201 Personal Identity Verification (PIV) of Federal Employees and Contractors (44 U.S.C. 3542(b)(2)). Other governing laws and regulations for managing and processing Federal credentials are as follows: 5 U.S.C. 301; Federal Information Security Act (P.L.104–106, sec. 5113); Electronic Government Act (P.L. 104–347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501); Government Paperwork Elimination Act (P.L. 105–277, 44 U.S.C. 3504); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; and Federal Property and Administrative Act of 1949, as amended OMB Circular No. A-130, Management of Federal Information Resources (11/28/2000) and Federal Agency Responsibilities for Maintaining Records about Individuals, dated June 25, 1993 (58 FR 36075, July 2, 1993); OMB Memo M-05-24, Federal Information Systems Management Act of 2002; and Executive Order -- Improving Critical Infrastructure Cyber Security (February 12, 2013).

PURPOSE(S): DIAMS will provide centralized, automated functionality to manage the many digital identities that interact with HUD's information technology environment. DIAMS will provide a central repository and web-based portal that stores and allows central management of core digital identification, credential and access management (ICAM) data elements. DIAMS

captures and stores information about persons and non-person entities that are granted access into HUD's business applications. DIAMS also provides HUD with a platform to centrally and actively manage the identity life-cycle of persons and non-person entities from account creation through account removal. DIAMS will integrate with HUD's authoritative data sources including HUD's human resource management system, physical access control system including USAccess operated by the General Services Administration, personnel clearance system, and multiple internal Directory Services to ensure synchronization of identities across HUD's digital landscape. DIAMS will use batch files and IdM's (Identity Management's) connector to synchronize data from and to authorized data sources. The connection pipe will be secured with Public Key Infrastructure exchange. A feed from HUD's Human Resource (HR) system for employees and Sponsor initiation of Contractors in IdM will start the on-boarding process for a HUD Identity. The on-boarding process will require notifications to the responsible manager or sponsor during all stages of the workflow. During employment, application access will be requested through the IdM application provisioning and de-provisioning functions by authorized HUD personnel. When personnel are off-boarded, HR and Sponsors will initiate off-boarding disabling accounts and removing privileges.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES. In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside HUD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To HUD contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement with HUD, when necessary

to accomplish an agency function or other activity related to this system of records, limited to only those data elements considered relevant to accomplishing an agency function. Individuals provided information under this routine use is subject to the same Privacy Act requirements and limitations on disclosure as are applicable to HUD officers and employees;

2. To appropriate agencies, entities, and persons to the extent such disclosures are compatible with the purpose for which the records in this system were collected, as set forth by Appendix I² – HUD’s Library of Routine Uses published in the Federal Register on (77 FR 41996, July 17, 2012);

3. To USAccess operated by the General Services Administration, personnel clearance system, and multiple internal Directory Services to ensure synchronization of identities across HUD’s digital landscape. DIAMS will share UPN and Email with USAccess;

4. To appropriate agencies, entities, and persons when: a) HUD suspects or has confirmed that the security or confidentiality of information in a system of records has been compromised; b) HUD 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 systems or programs (whether maintained by HUD or another agency or entity) that rely upon the compromised information; and c) 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 compromise and prevent, minimize, or remedy such harm for purposes of facilitating responses and remediation efforts in the event of a data breach;

² <http://portal.hud.gov/hudportal/documents/huddoc?id=append1.pdf>

5. To the National Archives and Records Administration (NARA) or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906; and

6. To other agencies to notify them when a PIV Card is no longer valid. The full system of records notice covering categories of DIAMS with complete description of other routine uses was published in the Federal Register: GSA GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS), 71 FR 56983 (September 28, 2006).

STORAGE: All data are stored at a secured data center on the production DIAMS database servers. Backup, recovery and archived digital media is stored in secure facilities located with Iron Mountain. There are no hardcopy records produced that require additional storage.

RETRIEVABILITY: Personnel information within the system is retrieved based on Name, Date of Birth and Social Security Numbers (SSNs), HUD Network ID, Home Address, US Citizenship. There are no hardcopy records produced that require additional retrieval.

SAFEGUARDS: The data in DIAMs records are backed up regularly in accordance with HUD policy 4.3.9 as documented in HUD Handbook 2400.25 Rev.3, August 2013. Strict access controls are governed for electronic records by the use of a user ID and password that require authentication before access is granted to DIAMS. Multi-factor authentication, once implementation is completed will require the use of PIV cards to access the system. Personnel who have access to the data are vetted by Personnel Security Division prior to being granted access to systems where sensitive Personally Identifiable Information (PII) resides, are provided PII training, and have access to all policies regarding PII and its safeguarding requirements. All database systems are housed in a secure data center that is protected by security personnel.

Accessing computer systems within the data center requires appropriate credentials to physically enter the facility and access the systems. All data is protected via encryption both at rest and in motion. There are no hardcopy records produced that require additional protections.

RETENTION AND DISPOSAL: Records retention and disposal are per Policy in HUD Handbook 2225.6 Rev 1 HUD Records Disposition Schedules Handbook (2225.6) Under General Records Schedule 24, Information Technology Operations and Management Records, Section 6 - User Identification, Profiles, Authorizations, and Password Files. Section 6 requires that files be destroyed/deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later. Backup and Recovery digital media will be destroyed or otherwise rendered irrecoverable per NIST SP 800-88 “Guidelines for Media Sanitization” (September 2006). This complies with all Federal regulations. There are no hardcopy records produced that require additional archival.

SYSTEM MANAGER(s) AND ADDRESS: Joseph Milazzo, Deputy Chief Information Officer for IT Operations, Department of Housing and Urban Development, 451 Seventh Street, SW, Room 4178, Washington, DC 20410.

NOTIFICATION AND RECORD ACCESS PROCEDURES: For Information, assistance, or inquiries about the existence of records, contact the Donna Robinson-Staton, Chief Privacy Officer, 451 Seventh Street, SW, Washington, DC 20410 (Attention: Capitol View Building, 4th Floor), telephone number: (202) 402-8073. Verification of your identity must include original signature and be notarized. Written request must include the full name, Social Security Number, date of birth, current address, and telephone number of the individual making the request.

CONTESTING RECORD PROCEDURES: The Department's rules for contesting contents of records and appealing initial denials appear in 24 CFR Part 16. Additional assistance may be obtained by contacting: U.S. Department of Housing and Urban Development, Chief Privacy Officer, 451 Seventh Street, SW, Washington, DC 20410 or the HUD Departmental Privacy Appeals Officers, Office of General Counsel, Department of Housing and Urban Development, 451 Seventh Street, SW, Washington DC 20410.

RECORD SOURCE CATEGORIES: The source of DIAMS records are Internal and External both. Internally sourced records come from HUD's Human Resource Systems, HUD's Physical Access Control System commonly referred to as Hirsch Velocity, HUD's systems maintaining personnel security records, and HUD's multiple Directory Services including Active Directory. Externally sourced records are from the General Service Administration's USAccess system.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT: None.