Mailing List

If you wish to be placed on the project mailing list to receive future or further information as the EIS process develops, contact Herrera at the address noted above.

Dated: April 6, 2000.

L. Jay Pearson,

Regional Administrator (10A).

[FR Doc. 00–9376 Filed 4–13–00; 8:45 am]

BILLING CODE 6820–23–M

GENERAL SERVICES ADMINISTRATION

Office of Communications; Cancellation of a Standard Form

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: The following Standard Form is cancelled because of low usage: SF 1012A, Travel Voucher (Memorandum).

DATES: Effective April 14, 2000.

FOR FURTHER INFORMATION CONTACT: Ms. Barbara Williams, General Services Administration, (202) 501–0581,

Dated: April 4, 2000.

Barbara M. Williams,

Deputy Standard and Optional Forms Management Officer.

[FR Doc. 00–9377 Filed 4–14–00; 8:45 am]

BILLING CODE 6820–34–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Privacy Act of 1974; New System of Records

AGENCY: National Institutes of Health, HHS.

ACTION: Notification of a new system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, the National Institutes of Health (NIH) is proposing to establish a new system of records, 09–25–0216, ''Administration: NIH Electronic Directory, HHS/NIH.''

DATES: NIH invites interested parties to submit comments concerning the proposed internal and routine uses on or before May 15, 2000. NIH has sent a report of a New System to the Congress and to the Office of Management and Budget (OMB) on April 3, 2000. This system of records will be effective May 24, 2000 unless NIH receives comments on the routine uses, which would result in a contrary determination.

ADDRESSES: Please submit comments to: NIH Privacy Act Officer, 6011 Executive Boulevard, Room 601, MSC 7669, Rockville, MD 20892, 301–496–2832. (This is not a toll free number.) Comments received will be available for inspection at this same address from 9 a.m. to 3 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: NIH Privacy Act Officer, 6011 Executive Boulevard, Room 601, MSC 7669, Rockville, MD 20892, 301–496–2832, (This is not a toll free number.)

SUPPLEMENTARY INFORMATION: The National Institutes of Health (NIH) proposes to establish a new system of records: 09–25–0216, ''Administration: NIH Electronic Directory, HHS/NIH.'' The purpose of the NIH Electronic Directory system of records is to support e-government; allow effective controls over the creation, maintenance and use of records in the conduct of current business; provide for effective management of costs, operation and interconnectivity of NIH information systems; provide the required structure for network security; and provide an accurate source of directory information at the NIH.

This system of records will allow the NIH to reliably identify individuals and manage the federal resources and authorities assigned to them, *e.g.*, organizational telephone numbers, addresses, and security authorizations. A single 10-digit NIH unique identifier (UID) will be assigned to each individual to permit association of a single person with descriptive information and resources throughout their career. It will allow creation of accurate records for individuals in the NIH directory and ensure that duplicate data files are compared, corrected and combined for accuracy, thus eliminating redundancy and general errors in identification.

Data collected is used to build an NIH centralized source identification directory and provides for directory security, system authentication and authorization. This system supports NIH corporate business processes and electronic commerce. Other Privacy Act systems of records that utilize this system as a source or confirmation for identification information will show this system as a records source.

The records in this system will be maintained in a secure manner compatible with their content and use. NIH staff will be required to adhere to the provisions of the Privacy Act, HHS Privacy Act Regulations, and the requirements of the DHHS Automated Information Systems Security Program Handbook.

Records may be stored on electronic media and as hard-copy records. Manual and computerized records will be maintained in accordance with the standards of Chapter 45–13 of the HHS General Administration Manual, ''Safeguarding Records Contained in Systems of Records,'' supplementary Chapter PHS hf: 45–13, and the Department's Automated Information System Security Program Handbook.

The following notice is written in the present, rather than future tense, in order to avoid the unnecessary expenditure of public funds to republish the notice after the system has become effective.

Dated: April 3, 2000.

Anthony L. Itteilag,

Deputy Director for Management, NIH.

SYSTEM NAME:

Administration: NIH Electronic Directory, HHS/NIH.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Records are maintained in databases located within the NIH computer facilities and the files of NIH functional offices required to identify individuals in order to manage the federal resources and authorities assigned to them. A current list of sites, including the address of any Federal Records Center where records from this system may be stored, is available by writing the System Manager listed under Notification Procedures below.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Users of NIH resources and services including but not limited to: current and past NIH employees, contractors, tenants of NIH facilities, participants in the NIH visiting programs, registered users of NIH computer facilities, grantees, reviewers, council members, collaborators, vendors, and parking permit holders. This system does not cover patients and visitors to the NIH Clinical Center.

CATEGORIES OF RECORDS IN SYSTEM:

This system is a source system that provides identification data to a variety of directory services at NIH that share comparable information and assign or relate dedicated federal resources to individuals. This system provides for a central directory that allows NIH to manage NIH corporate business processes and electronic commerce. The types of personal information in this directory are necessary to ensure the accurate identification of individuals

doing business in or with the National Institutes of Health. The types of personal information included in this directory are: Name, alias names, date of birth, place of birth, Social Security Number, gender, home address, home phone number, home FAX number, personal pager number, personal mobile phone number, personal email address, emergency contacts, photograph, digitized written signature, digitized biometrics, and NIH-assigned unique identifier. Public data refers to non-sensitive information readily available to the general public (*e.g.*, name, building, room number, and work phone). Non-public data refers to sensitive/confidential information or data for which access is limited to appropriate staff with a valid need-to-know in the performance of their official job duties, or as outlined in the routine uses for disclosure (*e.g.*, SSN, gender, home address, date of birth, place of birth).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301 and 302, 44 U.S.C. 3101 and 3102, Executive Order 9397.

PURPOSE:

The purpose is to establish a consolidated and centrally coordinated electronic directory to support e-government of administrative business processes; allow effective controls over the creation, maintenance and use of records in the conduct of current business; provide for effective management of costs, operation and interconnectivity of NIH information systems; provide the required structure for network security; and provide an accurate source of directory information at the NIH. Data collected is used to build an NIH centralized source identification directory and provides for directory security system authentication and authorization and supports NIH corporate business processes and electronic commerce. This system of records enables NIH to reliably identify individuals and those federal resources assigned to them. A NIH unique identifier (UID) will be assigned to each individual to permit identification of a single person with their descriptive information and resources throughout their career.

This system allows for the creation of accurate records for individuals in the NIH directory and ensures that duplicate data files are compared, corrected and combined for accuracy, thus eliminating redundancy. It is the central point of coordination for other automated systems that manage or track resources, particularly information security systems.

INTERNAL USE AND ACCESS TO PERSONAL INFORMATION:

Internal use and access to the personal information in this system will be limited to those with a valid need-to-know in the performance of their official duties. Typical internal uses of the system, including categories of users, uses of the data collected and the need for such use are as follows:

- Trans-NIH Human Resource Personnel, Administrative Officers, and administrative technicians, will access all public and non-public records for employees and/or NIH affiliates within their scope of responsibility to access/track staffing information such as personal/work contact information, physical location, and/or any other information to facilitate current NIH administrative business processes.
- Information Resources Management staff and Space and Facility Management personnel will have access to view public data (building location and work phone information) to coordinate access for, and the allocation of, telecommunication resources and building space/access.
- Supervisors, Administrative Officers and Administrative Technicians will have access to emergency contact information to enable them to contact someone in the event of an emergency.
- NIH central services staff, NIH police, and NIH management will access both public and non-public data to coordinate/track employee data required for other NIH business processes such as card key access, ID badges, parking permits, library resources, census information gathered for reporting requirements, employee development, training, campus security, and other administrative processes.
- NIH Security Officers, or other incident response personnel will have access to public/non-public data where NIH deems it necessary for official investigations or security incidents involving suspected intrusion, illegal activity, or unauthorized/unethical misuse of the system of records or data therein.

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

1. Disclosure may be made to a congressional office from the records of an individual in response to an inquiry from the congressional office made at the request of that individual.

2. Disclosure may be made to representatives of the General Services Administration or the National Archives and Records Administration who are conducting records management inspections under the authority of 44 U.S.C. 2904 and 2906.

3. Disclosure may be made to agency contractors, experts, consultants, or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients are required to maintain Privacy Act safeguards with respect to these records.

4. Disclosure may be made to respond to a Federal agency's request made in connection with the hiring or retention of an employee, the letting of a contract or issuance of a security clearance, grant, license, or other benefit by the requesting agency, but only to the extent that the information disclosed is relevant and necessary to the requesting agency's decision on the matter.

5. Disclosure may be made to the Department of Justice, or to a court or other adjudicative body, from this system of records when: (a) HHS, or any component thereof; or (b) any HHS officer or employee in his or her official capacity; or (c) any HHS officer or employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the officer or employee; or (d) the United States or any agency thereof where HHS determines that the proceeding is likely to affect HHS or any of its components, is a party to the proceeding or has any interest in the proceeding, and HHS determines that the records are relevant and necessary to the proceeding and would help in the effective representation of the governmental party.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN SYSTEM

STORAGE:

Records are maintained on electronic media such as computer tape and disk and/or hard-copy. Automated records are stored in controlled computer areas. Both manual and computerized records will be maintained in accordance with the standards of Chapter 45–13 of the HHS General Administration Manual, ''Safeguarding Records Contained in Systems of Records'', supplementary Chapter PHS hf: 45–13, and the Department's Automated Information System Security Program Handbook.

RETRIEVABILITY

Records are indexed and retrieved by: name, unique identifier, alias names, and social security number.

SAFEGUARDS:

1. *Authorized Users:* Non-public data on computer files is accessed by keyword known only to authorized users who are NIH employees or contractor staff who have a legitimate operational responsibility to access the data in the performance of their duties as determined by the System Manager. Staff are only granted access to those directories or fields for which they have operational responsibilities. User activity is recorded. Occurrences of non-routine user or operator activity are recorded. Public data is controlled by user-defined view via a web-based look-up table. View of public data is accessible and controlled via the NIH network.

2. *Physical Safeguards:* Physical access to the computer systems where records are stored is controlled through the use of door locks and alarms.

3. *Procedural and Technical Safeguards:* Access to the non-public data will be controlled through: password protection, user authentication, and system administration procedures for user access. User name and password authentication procedures are in place to protect non-public data from public view, and to prevent unauthorized personnel from accessing data. Logical access controls, based on job function, are in place to authorize and/or restrict the user activity and view of the data. Persons having access to data are restricted to a field-by-field confined user interface that permits a controlled, or narrow ''view'' of the data. Sensitive data transferred between NIH source databases is secured through encryption or similar manner. Digital certificates and automated user audit trail capabilities have been incorporated to ensure data integrity and to detect evidence of data tampering.

These practices are in compliance with standards of Chapter 45–13 of the HHS General Administration Manual, ''Safeguarding Records Contained in Systems of Records'', supplementary Chapter PHS hf: 45–13, and the Department's Automated Information Systems Security Program Handbook.

RETENTION AND DISPOSAL:

Records may be retired to a Federal Records Center and subsequently disposed of in accordance with the NIH Records Control Schedule. The Records Control Schedule and disposal standard for these records may be obtained by writing to the System Manager at the address below.

SYSTEM MANAGER(S) AND ADDRESS:

NIH Privacy Act Officer, 6011 Executive Blvd., Suite 601, MSC 7669, Rockville, MD 20892.

NOTIFICATION PROCEDURES:

Write to the System Manager listed above. The requester must verify his or her identity by providing either a notarization of the request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Act, subject to a five thousand-dollar fine. The request should include (a) Full name, and (b) address, and (c) year of records in question.

RECORD ACCESS PROCEDURES:

Write to the System Manager specified above to attain access to records and provide the same information as is required under the Notification Procedures. Requester should also reasonably specify the record content being sought. Individuals may also request an accounting of disclosure of their records, if any.

CONTESTING RECORDS PROCEDURES:

Address a petition for amendment to the System Manager. All requests must be in writing. The individual must identify himself/herself, specify the system of records from which the records are retrieved, the particular records to be corrected or amended, whether seeking an addition to or a deletion or substitution for the records, and the reason for requesting correction or amendment of the record.

RECORD SOURCE CATEGORIES:

NIH employees, contractors, and other persons who are using or performing services on behalf of the NIH, and the NIH human resource databases (*i.e.,* Human Resource Database (HRDB), Fellowship Payment System (FPS), J.E. Fogarty Database of Foreign Visiting Scientists (JEFIC), NIH Telecommunications Database (TELCOM), Parking and Identification Database (PAID), Email Directory and Forwarding Service (PH directory), and the Integrated Time and Attendance System (ITAS)).

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 00–9186 Filed 4–13–00; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–4561–N–24]

Notice of Submission of Proposed Information Collection to OMB; Evaluation of the Housing Opportunities for Persons With AIDS (HOPWA) Program

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notice.

SUMMARY: The proposed information collection requirement described below has been submitted to the Office of Management and Budget (OMB) for review, as required by the Paperwork Reduction Act. The Department is soliciting public comments on the subject proposal.

DATES: *Comments Due Date:* May 15, 2000.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Comments should refer to the proposal by name and/or OMB approval number and should be sent to: Joseph F. Lackey, Jr., OMB Desk Officer, Office of Management and Budget, Room 10235, New Executive Office Building, Washington, DC 20503.

FOR FURTHER INFORMATION CONTACT: Wayne Eddins, Reports Management Officer, Department of Housing and Urban Development, 451 7th Street, Southwest, Washington, DC 20410, e-mail Wayne__Eddins@HUD.gov; telephone (202) 708–2374. This is not a toll-free number. Copies of the proposed forms and other available documents submitted to OMB may be obtained from Mr. Eddins.

SUPPLEMENTARY INFORMATION: The Department has submitted the proposal for the collection of information, as described below, to OMB for review, as required by the Paperwork Reduction Act (44 U.S.C. Chapter 35). The Notice lists the following information: (1) the title of the information collection proposal; (2) the office of the agency to collect the information; (3) the OMB approval number, if applicable; (4) the description of the need for the information and its proposed use; (5) the agency form number, if applicable; (6) what members of the public will be affected by the proposal; (7) how