

(2) By delivery to room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

(3) By fax to the Docket Management Facility at 202-493-2251.

(4) Electronically through the Web Site for the Docket Management System at <http://dms.dot.gov>.

The Docket Management Facility maintains the public docket for this notice. Comments and material received from the public, as well as documents mentioned in this notice as being available in the docket, will become part of this docket and will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at <http://dms.dot.gov>.

Copies of the complete ICR are available through this docket on the Internet at <http://dms.dot.gov>, and also from Commandant (CG-611), U.S. Coast Guard Headquarters, room 6106 (Attn: Ms. Barbara Davis), 2100 2nd Street, SW., Washington, DC 20593-0001. The telephone number is 202-475-3523.

FOR FURTHER INFORMATION CONTACT: Ms. Barbara Davis, Office of Information Management, telephone 202-475-3523, or fax 202-475-3929, for questions on these documents; or telephone Ms. Renee V. Wright, Program Manager, Docket Operations, 202-493-0402, for questions on the docket.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

We encourage you to respond to this request for comments by submitting comments and related materials. We will post all comments received, without change, to <http://dms.dot.gov>; they will include any personal information you have provided. We have an agreement with DOT to use the Docket Management Facility. Please see the paragraph on DOT's "Privacy Act Policy" below.

Submitting comments: If you submit a comment, please include your name and address, identify the docket number [USCG-2006-25800], indicate the specific section of the document to which each comment applies, and give the reason for each comment. You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**; but

please submit them by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period. We may change the documents supporting this collection of information or even the underlying requirements in view of them.

Viewing comments and documents: To view comments, as well as documents mentioned in this notice as being available in the docket, go to <http://dms.dot.gov> at any time and conduct a simple search using the docket number. You may also visit the Docket Management Facility in room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street, SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Privacy Act: Anyone can search the electronic form of all comments received in dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the Privacy Act Statement of DOT in the **Federal Register** published on April 11, 2000 (65 FR 19477), or you may visit <http://dms.dot.gov>.

Information Collection Request

Title: Certificate of Discharge to Merchant Mariners.

OMB Control Number: 1625-0012.

Summary: Under 46, U. S. C. 10311, the Coast Guard prescribes the form of the Certificate of Discharge for Merchant Mariners. The Certificate provides merchant mariners with evidence of sea service to determine eligibility for various benefits, such as medical and retirement. The information collected is also used to show eligibility for an original, renewed, upgraded license or merchant mariner document, to develop maritime sea service statistics, and to provide information to the U.S. Maritime Administration (MARAD) on the availability of mariners in a time of national emergency. The Coast Guard's Sea Service database captures the information from the Certificates of Discharge and is used by the Coast Guard's Regional Examination Centers to evaluate the qualifications of mariners who apply for originals, renewals, upgrades to their license or merchant mariners documents. The information from the database is

compiled annually by MARAD to prepare Congressionally mandated reports on mariner availability. Currently, the CG Form 718A is only available in booklet format utilizing carbon copies. The Coast Guard is revising this form so that it may be provided to the maritime community for downloading via the internet. The new version still requires vessel master and discharged mariner signatures. This effort is intended to alleviate issues regarding form availability.

Need: The information is used primarily, on an as-needed basis, by mariners and the Coast Guard to establish sea service time and qualifications for issuing original, renewals or upgraded merchant mariner credentials; in claims against employers; in medical claims; and in qualifying for retirement benefits or insurance benefits.

Respondents: Masters or mates of shipping companies and merchant mariners.

Frequency: On occasion.

Burden Estimate: The estimated burden has decreased from 4,500 hours to 1,800 hours a year.

Dated: September 13, 2006.

R. T. Hewitt,

Rear Admiral, U.S. Coast Guard, Assistant Commandant for Command, Control, Communications, Computers and Information Technology.

[FR Doc. E6-15494 Filed 9-18-06; 8:45 am]

BILLING CODE 4910-15-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-4922-N-21]

Privacy Act of 1974; Amendment to Existing Privacy Act Systems, Employee Identification Files, HUD/Dept-71

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notification of an amendment to an existing System of Records, Employee Identification Files, HUD/Dept-71.

SUMMARY: HUD is completely revising HUD/Dept-71 to implement Homeland Security Presidential Direction 12 (HSPD-12) policy for a common identification standard for Federal employees and contractors. All of the sections including the system name are revised to reflect the current information requirements for individuals and contractors who require ongoing access to HUD's facilities and information technology systems.

DATES: *Effective Date:* This proposal shall become effective without further notice October 19, 2006 unless comments are received during or before this period which would result in a contrary determination.

Comments Due Date: October 19, 2006.

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

Communications should refer to the above docket number and title.

Facsimile (FAX) comments are not acceptable. A copy of each communication submitted will be available for public inspection and copying between 8 a.m. and 5 p.m. weekdays at the above address.

FOR FURTHER INFORMATION CONTACT: Jeanette Smith, Departmental Privacy Act Officer, telephone number (202) 708-2374. [This is not a toll-free number.] A telecommunications device for hearing and speech-impaired persons (TTY) is available at (800) 877-8339 (Federal Information Relay Services). [This is a toll-free number.]

SUPPLEMENTARY INFORMATION: The primary purposes of the system of records are:

(a) To ensure the safety and security of HUD facilities, systems, or information, and our occupants and users;

(b) To verify that all persons entering Federal facilities or using Federal information resources are authorized to do so;

(c) To track and control Personal Identity Verification (PIV) cards issued to persons entering and exiting the facilities, or using information systems.

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, notice is given that HUD proposes to amend an existing Privacy System of Records, Employee Identification Files HUD/Dept-71.

Title 5 U.S.C. 552a(e)(4) and (11) provide that the public be afforded a 30-day period in which to comment on the new record system. The new system report was submitted to the Office of Management and Budget (OMB), the Senate Committee on Governmental Affairs, and the House Committee on Government Reform pursuant to paragraph 4c of Appendix 1 to OMB Circular No. A-130, "Federal Responsibilities for Maintaining Records About Individuals," July 25, 1994 (59 FR 37914).

Accordingly, this notice amends HUD/Dept-71 system of records for the Office of Administration and accompanying routine uses to be submitted and accessed in the management of the Identity Management System by the Office of Administration.

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

Dated: September 12, 2006.

Ed Dorris,

Deputy Chief Information Officer, Office of Systems Integration and Efficiency.

DEPT/DEPT-71

SYSTEM NAME:

Identity Management System (IDMS).

SYSTEM LOCATION:

Data covered by this system are maintained at the following locations: U.S. Department of Housing and Urban Development (HUD), Office of Security and Emergency Planning (OSEP), 451 Seventh Street, SW., Washington, DC 20410. Some data covered by this system is at HUD Regional and Field Office locations, both Federal buildings and Federally-leased space, where staffed guard stations have been established in facilities that have installed the Personal Identity Verification (PIV) system, as well as the physical security office(s) or computer security offices of those locations.

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:

Individuals (employees or contractors) who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security, including applicants for employment or contracts, Federal employees, contractors, students, interns, volunteers, affiliates, and individuals formerly in any of these positions. The system also includes individuals authorized to perform or use services provided in HUD facilities (*e.g.*, Credit Union, Fitness Center, etc.). The system does not apply to occasional visitors or short-term guests to whom HUD will issue temporary identification and credentials.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained on individuals issued credentials by HUD include the

following data fields: Full name, Social Security number; date of birth; signature; image (photograph); fingerprints; hair color; eye color; height; weight; organization/office of assignment; company name (for contractors); telephone number; copy of background investigation form (Standard Form 85 or 85P or 86); PIV card issue and expiration dates; personal identification number (PIN) for the PIV Card; results of background investigation; PIV request form; PIV registrar approval signature; PIV card serial number; emergency responder designation; copies of documents used to verify identification or information derived from those documents (such as document title, document issuing authority, document number, document expiration date, document other information); level of national security clearance and expiration date; computer system user name; user access and permission rights, authentication certificates; and digital signature information.

Records maintained on PIV card holders entering HUD facilities or using HUD systems may include: Full name; PIV Card serial number; date, time, and location of entry; company name (for contractors); card expiration date; digital signature information; and computer networks/applications/data accessed.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); Government Paperwork Elimination Act (Pub. 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.

PURPOSE:

The primary purposes of the system of records are: (a) To ensure the safety and security of HUD facilities, systems, or information, and our occupants and users; (b) to verify that all persons entering Federal facilities or using Federal information resources are authorized to do so; (c) to track and control PIV cards issued to persons entering and exiting the facilities, or using information systems.

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

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 552a(b), and:

(1) To the Department of Justice when:

(a) The agency or any component thereof; or

(b) Any employee of the agency in his or her official capacity;

(c) Any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or

(d) The United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

(2) To a court or adjudicative body in a proceeding when:

(a) The agency or any component thereof;

(b) Any employee of the agency in his or her official capacity;

(c) Any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or

(d) The United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

(3) Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, 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, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with 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.

(4) To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

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

(6) To HUD contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

(7) To a Federal, State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.

(8) To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

(9) 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 approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

(10) To notify another Federal agency when, or verify whether, a PIV card is no longer valid.

(11) To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of

personal privacy, consistent with Freedom of Information Act standards.

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

STORAGE:

Records are stored in electronic media and in paper files. Paper files are kept in file folders or card files. Automated records are maintained in HUD's Security Control Access Tracking System (SCATS), and the DSX card access control system for HUD Headquarters.

RETRIEVABILITY:

Records are retrievable by last name, Social Security number, other ID number, PIV card serial number, image (photograph), or fingerprint.

SAFEGUARDS:

Paper records are kept in locked cabinets in secure facilities. Access to them is restricted to individuals whose role requires use of the records. The computer servers in which records are stored are located in facilities that are secured by alarm systems and off-master key access. The computer servers themselves are password-protected. Access to individuals working at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the client PCs at the guard stations and badging office will be encrypted when HUD upgrades to a PIV-II compliant system in 2007. Backup tapes are stored in a locked and controlled room in a secure, off-site location.

An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

RETENTION AND DISPOSAL:

Records relating to persons' access covered by this system are retained in accordance with HUD Handbook 2228.2, General Records Schedule 18, Item 17, approved by the National Archives and Records Administration (NARA). Unless retained for specific, ongoing security investigations, records of access are maintained for five years and then destroyed. For other facilities, records are maintained for two years and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding *no later than* 90 days after deactivation.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Physical Security Division, Office of Security and Emergency Planning, 451 Seventh Street, SW., Washington, DC 20410. Phone: (202) 708-2914.

NOTIFICATION PROCEDURES:

An individual can determine if this system contains a record pertaining to him/her by sending a request in writing, signed, to Director, Physical Security Division, Office of Security and Emergency Planning, 451 Seventh Street, SW., Washington, DC 20410. Phone: (202) 708-2914.

When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, full name, date of birth, Social Security number, and home address in order to establish identity.

RECORDS ACCESS PROCEDURES:

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. Rules regarding access to Privacy Act records appear in 24 CFR part 16. If additional information or assistance is required, contact HUD's Privacy Act Officer in the Office of the Chief Information Officer, 451 Seventh Street, SW., Washington, DC 20410. Phone: (202) 708-2374.

CONTESTING RECORD PROCEDURES:

Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state

the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in 24 CFR part 16. If additional information or assistance is required, contact HUD's Privacy Appeals Officer in the Office of the General Counsel, 451 Seventh Street, SW., Washington, DC 20410.

RECORD SOURCE CATEGORIES:

Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other Federal agencies; contract employer; former employer.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E6-15491 Filed 9-18-06; 8:45 am]

BILLING CODE 4210-67-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-4922-N-22]

Privacy Act of 1974; New System of Records, Personnel Security Files

AGENCY: Office of the Chief Information Officer, HUD.

ACTION: Notification of a new Privacy Act System of Records, Personnel Security Files.

SUMMARY: HUD is creating a new Privacy Act System of Records, Personnel Security Files. The records in this system of records are used to document and support decisions regarding clearance for access to classified information, the suitability, eligibility, and fitness for service of applicants for federal employment and contract positions, including students, interns, or volunteers to the extent their duties require access to federal facilities, information, systems, or applications. The records may be used to document security violations and supervisory actions taken.

DATES: *Effective Date:* This proposal shall become effective without further notice in 30 calendar days, October 19, 2006, unless comments are received during or before this period which would result in a contrary determination.

Comments Due Date: October 19, 2006.

ADDRESSES: Interested persons are invited to submit comments regarding this notice to the Rules Docket Clerk, Office of General Counsel, Department of Housing and Urban Development,

451 Seventh Street, SW., Room 10276, Washington, DC 20410-0500.

Communications should refer to the above docket number and title.

Facsimile (FAX) comments are not acceptable. A copy of each communication submitted will be available for public inspection and copying between 8 a.m. and 5 p.m. weekdays at the above address.

FOR FURTHER INFORMATION CONTACT:

Jeanette Smith, Departmental Privacy Act Officer, telephone number (202) 708-2374. [This is not a toll-free number.] A telecommunications device for hearing and speech-impaired persons (TTY) is available at (800) 877-8339 (Federal Information Relay Services). [This is a toll-free number.]

SUPPLEMENTARY INFORMATION: Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, notice is given that HUD proposes to create a new Privacy Act System of Records, Personnel Security Files.

Title 5 U.S.C. 552a(e)(4) and (11) provide that the public be afforded a 30-day period in which to comment on the new record system. The new system report was submitted to the Office of Management and Budget (OMB), the Senate Committee on Governmental Affairs, and the House Committee on Governmental Reform pursuant to paragraph 4c of Appendix 1 to OMB Circular No. A-130, "Federal Responsibilities for Maintaining Records About Individuals," July 25, 1994 (59 FR 37914).

Accordingly, this notice creates a new system of records for the Office of Administration and accompanying routine uses to be submitted and accessed in the management of the Personnel Security Files.

Dated: September 12, 2006.

Ed Dorris,

Deputy Chief Information Officer, Office of Systems Integration and Efficiency.

HUD/ADMIN-6

SYSTEM NAME:

Personnel Security Files.

SYSTEM LOCATION:

HUD Headquarters.

SECURITY CLASSIFICATION:

Most personnel identity verification records are not classified. However, in some cases, records of certain individuals, or portions of some records, may be classified in the interest of national security.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who require regular, ongoing access to federal facilities,