

and supporting materials; applications for bonds and licenses, and other DHS/CBP memoranda.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g). Additionally, the Secretary has exempted this system pursuant to 5 U.S.C. 552a(k)(2) of the Privacy Act from subsections (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29799 Filed 12-18-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0109]

Privacy Act of 1974; United States Coast Guard—017 Federal Medical Care Recovery Act System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of records notices, the Department of Homeland Security is giving notice that it proposes to update and reissue the following legacy record system DOT/CG 577 Federal Medical Care Recovery Act Record System (April 11, 2000) as a Department of Homeland Security system of records notice titled United States Coast Guard Federal Medical Care Recovery Act. This system will allow the Department of Homeland Security/United States Coast Guard to collect and maintain Federal Medical Care Recovery Act claims. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been reviewed and updated to better reflect the Department of Homeland Security/United States Coast Guard's Federal Medical Care Recovery Act record system. This new system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before January 20, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS-2008-0109 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 1-866-466-5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change and may be read at <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: For general questions please contact: David Roberts (202-475-3521), Privacy Officer, United States Coast Guard. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS)/United States Coast Guard (USCG) have relied on pre-existing Privacy Act systems of records notices for the collection and maintenance of records that concern the USCG Federal Medical Care Recovery Act (FMCRA).

As part of its efforts to streamline and consolidate its record systems, DHS/USCG is updating and reissuing a DHS/USCG system of records under the Privacy Act (5 U.S.C. 552a) that deals with the FMCRA. This record system will allow DHS/USCG to collect and maintain records regarding the FMCRA. The collection and maintenance of this information will assist DHS/USCG in meeting its obligation to address FMCRA claims. FMCRA is a statute that requires DHS/USCG to pursue collection actions for medical care provided to its beneficiaries. The FMCRA statute allows DHS/USCG to join and start their own action to collect for the medical care and lost wages provided to the beneficiary.

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of

records notices, DHS is giving notice that it proposes to update and reissue the following legacy record system DOT/CG 577 Federal Medical Care Recovery Act Record System (65 FR 19475 April 11, 2000) as a DHS/USCG system of records notice titled Federal Medical Care Recovery Act. This system will allow DHS/USCG to collect and maintain FMCRA claims. Categories of individuals and categories of records have been reviewed, and the routine uses of this legacy system of records notice have been updated to better reflect the DHS/USCG's FMCRA record system. This new system will be included in the DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the FMCRA Files System of Records.

III. Health Insurance Portability and Accountability Act

This system of records contains individually identifiable health information. The Health Insurance Portability and Accountability Act of

1996, applies to most of such health information. Department of Defense 6025.18–R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this system of records notice.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system of records to the Office of Management and Budget and to Congress.

System of Records DHS/USCG–017

SYSTEM NAME:

United States Coast Guard—017
Federal Medical Care Recovery Act.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at USCG Headquarters in Washington, DC, in field locations, and at USCG health care facilities at which the USCG military personnel or eligible dependent receives treatment.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include active duty, reserve, and retired active duty, retired reserve, and their eligible dependents. Also included are insurance company employees, related legal staff, the alleged tortfeasor. Finally, individuals such as Search and Rescue victims, employees, volunteers, or others who are provided emergency care by the USCG.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Military personnel's name;
- Eligible dependent's name;
- Social Security number;
- Gender;
- Date of birth;
- Case number;
- Insurance company's name and representative's name;
- Legal firm's name and legal representative's name;
- Addresses;
- Telephone numbers;
- Correspondence, memoranda, and related documents concerning potential and actual FMCRA claims;
- Police reports;
- Witness statements;
- Court documentation;
- Basic contact information for insurance companies, legal staff, and tortfeasor;

- Copies of medical and dental treatment provided to the individual subject of the claim;
- Copies of medical bills associated with civilian care provided at government expense; and
- Automated data processing (ADP) records containing identifying data on individuals, unit of assignment and address, home address, the amount of the claim, the amount paid to the government on the claim, dates of correspondence sent, due dates of reply, claim number, date claim opened, and date claim closed.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; The Federal Records Act, 44 U.S.C. 3101; 14 U.S.C. 632.; 10 U.S.C. 1095, Uniformed Services Medical and Dental Care; 42 U.S.C. 2651 *et seq.*, Federal Medical Care Recovery Act. 3 CFR 25.131, 133.

PURPOSE(S):

The purpose of this system is to collect and maintain FMCRA claims for the government.

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

Note: For records of identity, diagnosis, prognosis, or treatment of any client/patient, irrespective of whether or when he/she ceases to be a client/patient, maintained in connection with the performance of any alcohol or drug abuse prevention and treatment function conducted, requested, or directly or indirectly assisted by any department or agency of the United States, shall, except as provided therein, be confidential and be disclosed only for the purposes and under circumstances expressly authorized in 42 U.S.C. 290dd–2. The results of a drug test of civilian employees may be disclosed only as expressly authorized under 5 U.S.C. 7301. These statutes take precedence over the Privacy Act of 1974 to the extent that disclosure is more limited. The Routine Uses set forth below do not apply to this information. However, access to the record by the individual to whom the record pertains is governed by the Privacy Act.

A. To medical personnel to the extent necessary to meet a bona fide medical emergency;

B. To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation provided that employees are individually identified;

C. To the employee's medical review official;

D. To the administrator of any Employee Assistance Program in which the employee is receiving counseling or treatment or is otherwise participating;

E. To any supervisory or management official within the employee's agency

having authority to take adverse personnel action against such employee; or

F. Pursuant to the order of a court of competent jurisdiction where required by the United States Government to defend against any challenge against any adverse personnel action. See 42 U.S.C. 290dd, 290ee, and Public Law 100–71, Section 503(e).

Note: For all other records besides those noted above, this system of records contains individually identifiable health information. The Health Insurance Portability and Accountability Act of 1996 applies to most of such health information. Department of Defense 6025.18–R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this system of records notice. Therefore, routine uses outlined below may not apply to such health information.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such

information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department 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 this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To attorneys and insurance companies involved in settling and litigating claims pursuant to Health Information Portability and Accountability Act.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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

STORAGE:

Records in this system are stored electronically or on paper in secure

facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

RETRIEVABILITY:

Name, social security number, case number, or address of military personnel or eligible dependent. Records can also be retrieved by attorney's or other parties' names.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

Records are retained at USCG Headquarters for 2 years; transferred to a Federal Records Center and retained for an additional 4 years, for a total of 6 years, and destroyed thereafter. (AUTH: GRS 1, Item 19.)

SYSTEM MANAGER AND ADDRESS:

Human Resources Management, United States Coast Guard, Headquarters, 2100 2nd Street, SW., Washington, DC 20593-0001.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to Human Resources Management, United States Coast Guard, Headquarters, 2100 2nd Street, SW., Washington, DC 20593-0001.

When seeking records about yourself from this system of records or any other USCG system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486.

In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the USCG may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See "Notification procedure" above.

CONTESTING RECORD PROCEDURES:

See "Notification procedure" above.

RECORD SOURCE CATEGORIES:

From the individual, or if a minor, the parent or guardian, and witnesses. Medical facilities (USCG, Department of Defense, Uniformed Services Treatment Facility, or Civilian Facility) where beneficiaries are treated. Injury investigations. Attorneys and insurance companies involved in the claim.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29800 Filed 12-18-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0150]

Privacy Act of 1974; U.S. Customs and Border Protection—015 Automated Commercial System, System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security proposes to update and reissue the following legacy record system, Treasury/CS.278 Automated