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

STORAGE:

The data is stored electronically at the National Data Center and other DHS Data Centers for current data and offsite at an alternative data storage facility for historical logs and system backups.

RETRIEVABILITY:

The data is retrievable by name, address, unique identifiers or in association with an enforcement report or other system document.

SAFEGUARDS:

All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a ''need to know''; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

TECS also monitors source systems for changes to the source data. The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations. TECS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive information security program.

Access to TECS is controlled through a security subsystem, which is used to grant access to TECS information on a ''need-to-know'' basis.

RETENTION AND DISPOSAL:

The majority of information collected in TECS is used for law enforcement and counterterrorism purposes. Records in the system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

The retention period for information maintained in TECS is seventy-five (75) years from the date of the collection of the information or for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. TECS collects information directly from authorized users.

SYSTEM MANAGER AND ADDRESS:

Assistant Commissioner, Office of Information Technology, Passenger Systems Program Office, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, CBP will consider individual requests to determine whether or not information may be released. Thus, 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 CBP's FOIA Officer, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

When seeking records about yourself from this system of records or any other CBP 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 CBP 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:

This system contains investigatory material compiled for law enforcement and counterterrorism purposes whose sources need not be reported.

EXEMPTIONS CLAIMED FOR THE 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). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). In addition, to the extent a record contains information from other exempt systems of records, CBP will rely on the exemptions claimed for those systems.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29807 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0140]

Privacy Act of 1974; United States Coast Guard–028 Family Advocacy Case Records 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 United States Coast Guard legacy record system DOT/CG 631 Family Advocacy Case Records System (April 11, 2000) as a Department of Homeland Security system of records notice titled Family Advocacy United States Coast Guard Case Records. This system will allow the Department of Homeland Security to administer the United States Coast Guard Family Advocacy Program. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been reviewed updated to better reflect the Department of Homeland Security/United States Coast Guard's—028 Family Advocacy Case Records system of records. Elsewhere in today's **Federal Register**, the Department is publishing a notice of proposed rulemaking to exempt this system of records from certain portions

of the Privacy Act. 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. This new system will be effective January 20, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0140 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) and United States Coast Guard (USCG) have relied on previous Privacy Act systems of records notices for the collection and maintenance of records that concern the USCG–028 Family Advocacy Case Records system of records.

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a DHS/USCG system of records under the Privacy Act (5 U.S.C. 552a) that deals with USCG Family Advocacy Program. The collection and maintenance of this information will assist DHS/USCG in meeting its obligation to administer the DHS/USCG Family Advocacy Program.

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 631 Family Advocacy Case Record System (65 FR 19476 April 11, 2000) as a DHS/USCG system of records notice titled DHS/USCG–028 Family Advocacy Case Records. This system will allow DHS/USCG to administer the USCG Family Advocacy Program. 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 DHS/USCG–028 Family Advocacy Case Records system of records. This new system will be included in 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. When information about an adult dependent is contained in a Family Advocacy Case Record, that dependent may request access to the record 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. Information about individuals, other than the individual requesting access, will be redacted.

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 Family Advocacy Case Records 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–028

SYSTEM NAME:

United States Coast Guard Family Advocacy Case Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the USCG Headquarters in Washington, DC, and servicing Work-Life Offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include active duty, reserve, and retired active duty and retired reserve military personnel and their dependents entitled to care at a USCG or other military or dental facility whose abuse or neglect is brought to the attention of appropriate authorities. Also included are persons suspected of abusing or neglecting such beneficiaries and persons presenting a need for preventive services.

CATEGORIES OF RECORDS IN THIS SYSTEM INCLUDE:

- Individual's name;
- Name of the suspected or confirmed abuser/neglecter or person in need of preventive services;
- Employee Identification Number and/or Social Security Number;
- Medical records of suspected and confirmed cases of family member abuse or neglect;
- Interviews and intake reports;
- Investigative reports;
- Correspondence;
- Family Advocacy Incident Determination Committee reports;

- Clinical assessment reports;
- State and/or local child protective services reports;
- Follow-up and evaluation reports; and
- Other supportive data assembled relevant to individual Family Advocacy Program files.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 14 U.S.C. 632; the Federal Records Act; 42 U.S.C. 5101, 5102; 44 U.S.C. 3101; COMDTINST 1750.7C.

PURPOSE(S):

The purpose of this system is to administer the USCG Family Advocacy program, including to maintain records that identify, monitor, track and provide treatment to alleged offenders, eligible victims and their families of substantiated spouse/child abuse and neglect; and to manage prevention programs to reduce the incidence of abuse throughout the USCG military communities.

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

Note: Disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act limit access to those individuals within the Coast Guard who have a ''need to know'' in order to perform their official duties. Confidential information contained in Family Advocacy Case Records should generally be limited to the servicing Family Advocacy Specialist, with access permissible to the Family Advocacy Program Manager and direct supervisor of the Family Advocacy Specialist, on a ''need to know'' basis. When direct and complete access to the record is given to any other personnel within the agency who does not have a ''need to know'' in order to perform their official duties, written permission of the service member and any identified adult dependent is required.

Note: 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 Federal, State, or local government or private agencies, or approved researchers for coordination of family advocacy programs, medical care, mental health treatment, and research into the causes and prevention of family domestic violence and trends within the USCG.

I. To Federal, State, or local governmental agencies when it is deemed appropriate to use civilian resources in counseling and treating individuals or families involved in child abuse or neglect or spouse abuse; or when appropriate or necessary to refer a case to civilian authorities for civil or criminal law enforcement; or when a state, county, or municipal child protective service agency inquires about a prior record of substantiated abuse for the purpose of investigating a suspected case of abuse.

J. To victims and witnesses of a crime for purposes of providing information consistent with the requirements of the Victim and Witness Assistance Program, regarding the investigation and disposition of an offense.

K. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

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 electronically on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Individual's name, social security number, types of incidents, employee identification number.

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 and/or paper files 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. Those individuals routinely granted full access are Family Advocacy Program staff. When appropriate, those individuals may share information with persons outside the Family Advocacy Program, which is generally limited to a summary of the incident; names of individuals involved, when appropriate; and overview of assessment, disposition and treatment recommendations.

RETENTION AND DISPOSAL:

Records are maintained at the servicing Work-Life Office until the case is closed or the service member is separated from the Coast Guard. Upon closure of the case or separation of the sponsor, the paper record will be transferred to Commandant, CG–1112, or retained at the servicing Work-Life Office. The record is retained for five years from case closure or last date of action. At the end of five years the record is destroyed, except for information concerning certain minor USCG dependents who are victims of child abuse, neglect, or sexual abuse. These records are retained until the dependent turns 18 years-old. (AUTH: N1–26–05–8, Items, 1, 2, 3)

SYSTEM MANAGER AND ADDRESS:

Commandant, CG–111, Office of Work-Life-WP, Director, Personnel Management Directorate, 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 Commandant, CG–111, Office of Work-Life G–WP, Director, Personnel Management Directorate, 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:

Reports from medical personnel, educational institutions, law enforcement agencies, public and private health and welfare agencies, USCG personnel and private individuals.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

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

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29808 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0128]

Privacy Act of 1974; Federal Emergency Management Agency—006 Citizen Corps Database 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 FEMA/VOL–1 Citizen Corps Database (April 29, 2002) as a Department of Homeland Security system of records notice titled, Federal Emergency Management Agency—006 Citizen Corps Database. 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's Federal Emergency Management Agency Citizen Corps Database. The Citizen Corps, through its internet site at *http://www.citizencorps.gov*, allows individuals to indicate their interest in specific voluntary programs. Information concerning those desired activities is then disseminated by DHS/FEMA to the appropriate organization for further processing or response. The Citizen Corps coordinates efforts among several organizations, including the Community Emergency Response Teams (CERT), the Fire Corps, the Office of the Civilian Volunteer Medical Reserve Corps (MRC), the National Neighborhood Watch Program, the Volunteers in Police Service (VIPS), the Operation Terrorism Information and Prevention System (TIPS), the Corporation for National and Community Service (CNCS), and the Citizen Corps Council. In addition, these entities may express an interest in sharing their respective contact and similar information with other participants in these programs. This