DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0068]

Privacy Act of 1974; Department of Homeland Security /United States Coast Guard – 002 Employee Assistance Program Records System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/United States Coast Guard Employee Assistance Program Records System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to administer the United States Coast Guard Employee Assistance Program for military personnel. As a result of the biennial review of this system, the system manager and address category has been updated. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0068 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Marilyn Scott-Perez (202) 475-3515, Privacy Officer, Commandant (CG-61), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) United States Coast Guard (USCG) proposes to update and reissue a current DHS system of records titled, "DHS/United States Coast Guard-002

Employee Assistance Program Records System of Records." The collection and maintenance of this information will allow the DHS/USCG to administer the United States Coast Guard Employee Assistance Program for military personnel. As a result of a biennial review of the system, the system manager and address category has been updated to reflect the new mail stop.

Consistent with DHS's information-sharing mission, information stored in the DHS/USCG-002 Employee Assistance Program Records System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice. This updated system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate 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 from 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 U.S. citizens and lawful permanent residents. As a matter of policy, DHS

extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCG-002 Employee Assistance Program Records System of Records.

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

System of Records

Department of Homeland Security (DHS)/USCG –002

System name:

DHS/USCG-002 Employee Assistance Program Records

Security classification:

Unclassified

System location:

Records are maintained at the United States Coast Guard Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

All USCG active duty, reserve, and retired active duty and reserve military personnel and their eligible dependents/individuals who have been referred for assistance or counseling, are being assisted or counseled, or have been assisted or counseled by the USCG Employee Assistance Program. Eligibility will vary based on status.

Categories of records in the system:

Categories of records in this system include:

- Military personnel's name;
- Eligible dependent/individual's name, if applicable;
- Social Security number;
- Employee identification number;
- Date of birth;
- Addresses;
- E-mail address;
- Telephone numbers;
- Job-related information including: job title; rank; duty station; supervisor's name and telephone number; documents received from supervisors or personnel regarding work place problems or performance; leave and attendance records; and workplace-related recommendations made to supervisors as a result of a team meeting;
- Counseling and intervention-related information including: notes and documentation of Employee Assistance Program counselors; records of treatment, including non-clinical educational interventions; counseling referrals; team reports; records of employee attendance at treatment and counseling programs; prognosis of individuals in treatment or counseling programs; insurance data; addresses and contact information of treatment facilities; name and address of individuals providing treatment or counseling or intervention; and Privacy Act notification forms and written consent forms;

- USCG Workplace Violence and related Critical Incident Team records of the Workplace Violence Prevention Program, maintained by USCG Work-Life personnel. These records may include written reports and recommendations to leadership personnel regarding alleged work place violence incidents;
- USCG Critical Incident Stress Management-related records, which may include descriptions of incidents, consultations, interventions, and may contain personally-identifying information (for the purpose of follow-on contacts with those thought to be impacted by the critical incident);
- USCG Sexual Assault Prevention and Response Program case records maintained by USCG Work-Life personnel. These records are used to facilitate services for victims and their family members as appropriate. In addition to information cited above, these records may contain Victim Reporting Preference Statement, case notes, and safety plan. Record may also contain descriptions of alleged assaults;
- USCG Victim Support Person or Victim Advocate maintained by USCG Work-Life personnel. These are maintained in conjunction with efforts to provide assistance to victims of crime. Records will contain signed Victim Support Person or Victim Advocate Statement of Understanding and Victim Support Person or Victim Advocate Supervisor;
- Statement of Understanding, assignment information, and notes regarding results of screening interview, relevant training received, and any other information relevant to the Victim Support Person's or Victim Advocate's provision of support services to victims;

- USCG Critical Incident Stress Management Peer Volunteers maintained by USCG Work-Life personnel. These records contain statement of understanding, notes regarding screening interview, record of related training received, and any other information relevant to the peer's provision of services when deployed after a critical incident;
- Case records maintained by USCG Work-Life personnel on USCG Active Duty members who have demonstrated suicidal behavior. The purpose of these records is to facilitate continuity of care for personnel who have exhibited suicidal behavior. These records will contain reports regarding each incident and follow-up case notes;
- Reports of USCG active duty suicidal behavior incidents, work place violence incidents, critical incidents, and sexual assaults are maintained by USCG Headquarters (CG-1112). These reports are received from Work-Life Offices, which are responsible for providing services for the related programs described above. Their purpose is to ensure continuity of care and to identify any systemic issues found in aggregate data.

Authority for maintenance of the system:

5 U.S.C. 7361, 7362, 7901, and 7904; 5 U.S.C. 301; Federal Records Act, 44 U.S.C. 3101.

Purpose(s):

The Employee Assistance Program will maintain information gathered by and in the possession of the USCG Employee Assistance Program, an internal agency program designed to assist employees of USCG and, in certain instances, their eligible dependents/individuals, in regard to a variety of personal and/or work related problems. The program involves counseling, educational, and consultative services provided through the internal and external Employee Assistance Program for alcohol, drug, emotional, or behavioral problems, and addresses mandatory and voluntary counseling following exposure to a traumatic incident, responses to critical incidents that impact employees, and workplace incidents involving actual violence or the threat of violence and necessary follow up.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Disclosure of substance abuse records is limited to the parameters set forth in 42 U.S.C. 290dd, 290ee, and Public Law 100-71, Section 503(e). Accordingly, a Federal employee's substance abuse records may not be disclosed without the prior written consent of the employee, unless the disclosure would be one of the following:

A. To the Department of Justice (including Offices of the United States Attorneys) 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 when 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 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 the Department or another agency or entity) or harm to the individual who relies upon the compromised information;

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

C. 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.

D. To appropriate State and local authorities to report, under State law, incidents of suspected child abuse or neglect to the extent described under 42 CFR 2.12.

E. To any person or entity to the extent necessary to prevent an imminent and potential crime that directly threatens loss of life or serious bodily injury.

F. To report to appropriate authorities when an individual is potentially at risk to harm himself or herself or others.

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

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

I. To the employee's medical review official.

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

K. To any supervisory or management official within the employee's agency having authority to take adverse personnel action against such employee.

L. Pursuant to the order of a court of competent jurisdiction when 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).

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

USCG stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media.

Retrievability:

USCG may retrieve records/data by a Military personnel's or eligible dependent's name. USCG Critical Incident Stress Management-related records are filed by unit name and are not retrievable by individual name, but instead, by unit name.

Safeguards:

USCG safeguards records in this system in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. USCG imposes strict controls to minimize the risk of compromising the information in this system. 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:

USCG maintains and disposes of records in accordance with National Archives and Records Administration-approved agency Records Schedule, SSIC 1754, item 1

(AUTH: N1-026-07-1, Item1) Employee Assistance Program (EAP) Coordinator Case Records; if not disclosed under the Privacy Act, records are retained for three years after the client has ceased contact and then destroyed.

Employee Assistance Program client records may contain Department of Transportation-required Substance Abuse evaluations and USCG Sexual Abuse Prevention and Response Program client records; if not disclosed under the Privacy Act, these are destroyed with the EAP Coordinator case records three years after the last contact with the client.

Employee Assistance Program Coordinator Case Records that USCG discloses are retained until five years after the client has ceased contact or, if later, for five years after last disclosure of information from the record, as authorized by General Records Schedule 14, item 23.

All records will be retained beyond their normal maintenance period until any pending litigation is completed. This will be true whether or not the client has terminated employment with DHS/USCG. Individual states may require longer retention. The rules in this system notice should not be construed to authorize any violation of such state laws that have greater restrictions.

USCG will destroy files only after the required period of maintenance, with a witness present, by either (1) a DHS or USCG Employee Assistance Program Administrator or an Employee Assistance Program Administrator from another organization that contracts with DHS or USCG for Employee Assistance Program services, or (2) by designated staff of a private or governmental organization under

contract with DHS or USCG to provide document destruction services. The witness must be trained in the proper handling of records covered by the Privacy Act and 42 CFR part 2.

USCG destroys written records by shredding or burning. USCG destroys records stored on hard drives using software tools that ensure the protection of the confidential information by making reconstruction or compromise by reuse impracticable. USCG disposes of records contained on back-up tapes/diskettes by either physically destroying the tapes/diskettes or by deleting them using software tools which ensure the protection of the confidential information by making reconstruction or compromise by reuse impracticable.

USCG transfers records located away from the destruction site in a confidential manner. No other information about Employee Assistance Program clients may be maintained once these files have been destroyed.

System Manager and address:

Commandant (CG-111), United States Coast Guard, Mail Stop 7907, Washington, D.C. 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 the Commandant (CG-611), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593.

If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental 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 Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and

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 the above information, the component(s) 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:

Records are retained from the following sources:

USCG Employee Assistance Program: the client, the licensed mental health provider, and collateral sources and resources intended to help the client;

USCG Workplace Violence and related Critical Incident Team: investigation records, personnel records, critical incident team assembled to make recommendations to command, subject's supervisors, and the subject;

USCG Critical Incident Stress Management-related records: Work-Life staff, Peers, Incident commander, command(s) affected, individuals impacted by incident, and other support persons who may be mobilized to assist those impacted by the event;

USCG Sexual Assault Prevention and Response Program: victim, victim support person, medical personnel assisting victim, criminal investigations and investigators, and other support personnel intended to assist victim;

USCG Victim Support Persons (VSP): the victim support person, Work-Life staff, VSP's or Victim Advocate's work supervisor, and other support persons who may assist in training;

USCG Critical Incident Stress Management Peer Volunteers: Peer, Peer's supervisor, Work-Life staff, and other support persons who may assist in training;

Case records maintained by USCG Work-Life personnel on USCG Duty members who have demonstrated suicidal behavior: the patient, medical personnel, patient's command, and Work-Life staff and other support persons who may assist in helping the patient; and

Reports of USCG active duty suicidal behavior incidents, work place violence incidents, critical incidents, and sexual assaults maintained by USCG Headquarters (CG-1112): Work-Life staff and others as described above under their related programs.

Exemptions claimed for the system:

None.

Dated: November 18, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

9110-04

[FR Doc. 2014-29379 Filed 12/15/2014 at 8:45 am; Publication Date: 12/16/2014]