

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, 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 the Commandant (CG-611), United States Coast Guard, Mail Stop 7710, Washington, DC 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 SW., Building 410, STOP-0655, Washington, DC 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.

[FR Doc. 2014-29379 Filed 12-15-14; 8:45 am]

BILLING CODE 9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0070]

Privacy Act of 1974; Department of Homeland Security/United States Coast Guard—016 Adjudication and Settlement of Claims 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 Adjudication and Settlement of Claims System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to collect and preserve the records associated with military personnel salary claims. As a result of the biennial review of this system, the system manager and address and record source categories have 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 January 15, 2015. This updated system will be effective January 15, 2015.

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0070 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, 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 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, DC 20593. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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—016 Adjudication and Settlement of Claims System of Records. The collection and maintenance of this information will assist DHS/USCG in meeting its statutory obligation to adjudicate and settle salary claims received by USCG military personnel. The DHS/USCG—016 Adjudication and Settlement of Claims System of Records is the USCG's record system used for the collection and maintenance of records that concern the adjudication and settlement of claims concerning the amounts of pay received by USCG military personnel. As a result of a biennial review of the system, the system manager and address and record

source categories have been updated to include the new command name, office symbol, and mail stop.

Consistent with DHS's information-sharing mission, information stored in the DHS/USCG—016 Adjudication and Settlement of Claims 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—016 Adjudication and Settlement of Claims 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—016

SYSTEM NAME:

DHS/USCG—016 Adjudication and Settlement of Claims System of Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

USCG maintains records at the United States Coast Guard Headquarters in Washington, DC and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include active duty, reserve, retired active duty, and retired reserve military personnel who submit claims against USCG related to monetary disputes.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Individual's name;
- Social Security number or Employee ID Number (EMPLID);
- Leave and earnings statements; and
- Other related information regarding claims arising out of disputes concerning amounts of pay received.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Departmental Regulations, 5 U.S.C. 301, 5512-5514; 10 U.S.C. 939, 1442, 1453, 2774-2775; 14 U.S.C. 461; 31 U.S.C. 3716; 37 U.S.C. 1007; the Federal Records Act, 44 U.S.C. 3101; Debt Collection Act of 1982, Public Law 97-276, Section 124; Debt Collection Improvement Act of 1996, Public Law 104-132; Federal Claims Collection Standards, 31 CFR Chapter IX.

PURPOSE(S):

The purpose of this system is to adjudicate and settle claims related to salary disputes, overpayments resulting from travel and transportation entitlement, claims from spouses, former spouses or widows of military personnel involving an annuity, and other similar activities when submitted by USCG active duty, reserve, and retired active duty and retired reserve military personnel.

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

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 or 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 (DOJ), 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 relevant or 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 or former employee of DHS in his/her official capacity;
3. Any employee or former 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.

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 (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization 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. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely 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, when 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 authorized officials of the Internal Revenue Service, General Accountability Office (GAO), and the Civil Service Commission, as required, to address salary claims submitted by USCG military and civilian personnel.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings or in response to a subpoena.

J. 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:

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 retrieves records by claimant's name, employee ID (EMPLID), or Social Security number.

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. 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 retains records until adjudication and settlement. USCG retains most submissions for present setting value, as required. USCG retains records for 10 years, 3 months after the year in which the Government's right to collect first accrued. (AUTH: GRS 6, Item 10b(2)(a))(Records Officer).

SYSTEM MANAGER AND ADDRESS:

Commandant (CG-12), United States Coast Guard, Mail Stop 7907, 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 the Commandant (CG-611), United States Coast Guard, Mail Stop 7710, Washington, DC 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 SW., Building 410, STOP-0655, Washington, DC 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:

USCG obtains records from individuals, USCG payroll offices, legal staff, investigators, Personnel Directorate, Comptroller General, GAO, and congressional correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: November 18, 2014.

Karen L. Neuman,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2014-29381 Filed 12-15-14; 8:45 am]

BILLING CODE 9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0071]

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

AGENCY: Department of Homeland Security, Privacy Office.

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 Federal Medical Care Recovery Act System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to collect and maintain Federal Medical Care Recovery Act claims (FMCRA). 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 January 15, 2015. This updated system will be effective January 15, 2015.

ADDRESSES: You may submit comments, identified by docket number DHS-2014-0071 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, 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 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, DC 20593. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 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-017 Federal Medical Care Recovery Act System of Records. The collection and maintenance of this information will assist DHS/USCG in meeting its statutory obligation to address FMCRA claims. 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-017 Federal Medical Care Recovery Act 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-017 Federal Medical Care Recovery Act 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-017

SYSTEM NAME:

DHS/USCG-017 Federal Medical Care Recovery Act.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Records are maintained at the United States Coast Guard Headquarters in Washington, DC and field offices and at USCG health care facilities where 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