9110-04

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0072]

Privacy Act of 1974; Department of Homeland Security /United States Coast Guard – 060 Homeport 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 Homeport System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to validate the suitability and identify the eligibility of those who request permission and/or have access to the system. 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-2014-0072 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-060

Homeport System of Records. The collection and maintenance of this information will assist DHS/USCG in meeting its maritime security requirements under the Maritime Transportation Security Act (MTSA) of 2002. As a result of a biennial review of the system, the system manager and address category has been updated to include the new office symbol, and mail stop.

Consistent with DHS's information-sharing mission, information stored in the DHS/USCG-060 Homeport 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-060 Homeport 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 –060

System name:

DHS/USCG-060 Homeport System of Records.

Security classification:

Classified, sensitive, and unclassified

System location:

Records are maintained at the United States Coast Guard Headquarters in Washington, D.C., the USCG Operations Systems Center, 600 Coast Guard Drive, Kearneysville, WV, and field offices. Homeport is the information technology (IT) system in which records associated with this function are maintained.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

Representatives of the maritime industry, such as: Members of Area Maritime Security Committees (AMSC); National Harbor Safety Committees and Environmental Committees (NHSCEC); and other entities regulated under the Maritime Transportation Security Act (MTSA).

Federal, State and local government agency members involved in maritime safety, security, and environmental protection missions. These persons may complete on-line forms and/or request an account to provide the information required by the USCG, access sensitive but unclassified information, and participate in collaboration communities.

Individuals for whom background screening will be conducted for the purpose of facilitating the establishment of AMSC membership and to inform owners, operators, and security officers of MTSA regulated entities of the names of persons who have passed the background screening including, but not limited to Owners and Operators and their employees, and non-employees who require regular access privileges to such regulated vessels and facilities, as well as many credentialed merchant mariners.

Categories of records in the system:

To participate in the Homeport portal for information dissemination and collection, the following information may be included in this record system:

- Full name;
- Complete address;
- Country;
- Company or organization name;
- Work phone;
- Mobile phone;
- 24 hour contact phone;
- Fax;
- Pager;

- E-mail address;
- Alternate e-mail address; and
- Referral full name/work and cell phone/e-mail address.

For USCG active duty and civilian personnel, the following fields are pre-populated using data from the Direct Access system, the USCG's enterprise human resource system:

- Employee ID;
- Billet control number;
- Government Service Grade or Military Rate/Rank; and
- Position number.

For purposes of establishing AMSC membership, the following information will be included in accordance with 33 CFR 103.305 "Composition of an Area Maritime Security (AMS) Committee:"

- Full name;
- Date of birth; and
- Alien identification number (if applicable).

For purposes of establishing Transportation Worker Identification Credential (TWIC) New Hire query, the following information will be included in accordance with Navigation and Vessel Inspection Circulars (NVIC) 03-07:

- Full name; and
- Social Security number (last 4 digits only) should it be provided (not required).

Authority for maintenance of the system:

46 U.S.C. 3717; 46 U.S.C. 12501; 44 U.S.C. 3507; 33 U.S.C. 1223; 50 U.S.C. 191; 14 U.S.C. 93(a) (6); and 33 CFR part 125.

Purpose(s):

The Homeport system is an enterprise tool that facilitates compliance with the requirements set forth in the Maritime Transportation Security Act (MTSA) of 2002, by providing secure information dissemination, advanced collaboration, electronic submission and approval for vessel and facility security plans, and complex electronic and telecommunication notification capabilities. The collection of personally identifiable information concerning those with access to the Homeport system allows the USCG to validate the suitability and identify the eligibility of those who request permission and/or have access to the system.

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 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 Homeport information 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 homeport records by first name, last name, city, state, Captain of the Port Zone, vessel role, facility role, committee membership, vessel association, case identification number, or facility association.

Safeguards:

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

In accordance with NARA disposition Authority Number N1-026-06-06, records of registration information are destroyed upon account termination. Maritime personnel screening data is destroyed after two years. Response-associated information, such as personal data needed for search and rescue purposes, is destroyed 120 days following completion of response operations.

System Manager and address:

Commandant (CG-633), United States Coast Guard, Mail Stop 7710, 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 obtained by registered users; the general public (if completing an on-line form during marine casualty incidents or natural disasters); individuals who are authorized to have access to maritime facilities; government agencies; and USCG personnel.

Exemptions claimed for the system:

None.

Dated: November 18, 2014.

Karen L. Neuman,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2014-29354 Filed 12/15/2014 at 8:45 am; Publication Date: 12/16/2014]