• An explanation of 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;

• 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 this bulleted 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. In addition, individuals in ICE-owned facilities or in contract detention facilities operated on behalf of ICE may request access to their records by making a request to the facility's health care unit. Specifically, individuals should submit a Form G–639, Freedom of Information/Privacy Act Request form, to any staff member.

ICE also detains individuals in Intergovernmental Service Agreement (IGSA) facilities. These facilities are city, county, or State-owned and operated facilities where ICE contracts for detention services or leases bed space. There is no set procedure for how individuals in the IGSA facilities request access to their records. Each facility has its own process. Persons seeking such information should contact the chief administrative officer of such facility for guidance.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Information may be obtained from the individual, immediate family members, physicians, nurses, dentists, medical laboratories and testing facilities, hospitals, other medical and dental care providers, other law enforcement or custodial agencies, and public health agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: November 2, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–26910 Filed 11–6–09; 8:45 am]

BILLING CODE 9111–28–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0114]

Privacy Act of 1974; Department of Homeland Security U.S. Coast Guard—060 Homeport System of Records

AGENCY: Privacy Office, DHS.

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 system of records notice titled, Department of Homeland Security/U.S. Coast Guard—060 Homeport System of Records. The updated system of records, Department of Homeland Security/U.S. Coast Guard—060 Homeport System of Records contains a secure collection of information from and about individuals and entities that are subject to the requirements of the Maritime Transportation Security Act of 2002. As a result of the biennial review of this system, the Department of Homeland Security U.S. Coast Guard is proposing changes to (1) the categories of individuals covered to include Federal, State and local government agency members involved in maritime safety, security and environmental protection missions; categories of records to include government service grade or military rate/rank, and for Transportation Worker Identification Credential new hire query, the addition of full name and optional social security number (last four; not required); (2) the purpose to state that the Homeport system will no longer be used to collect information from and about individuals for whom background screening will be conducted for purposes of establishing U.S. Coast Guard approved identification credentials for access to maritime facilities (records associated with this function have been deleted); and (3) the routine uses to conform with Department's library of routine uses. No new routine uses have been added. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before December 9, 2009. The updates to this system will be effective December 9, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2009–0114 by one of the following methods:

• *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *Fax:* 703–483–2999.

• *Mail:* Mary Ellen Callahan, 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 go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Sherry A. Richardson (202–475–3515), Privacy Officer, U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Homeland Security (DHS) U.S. Coast Guard (USCG) is revising a system of records under the Privacy Act of 1974 (5 U.S.C. 552a), for the DHS/USCG—060 Homeport System of Records. The Department is updating and reissuing the DHS/USCG—060 Homeport System of Records (71 FR 25203, April 28, 2006) to cover inclusion of these updated records. The collection and maintenance of this information will assist the USCG in meeting its maritime security requirements under the Maritime Transportation Security Act (MTSA) of 2002.

MTSA establishes a comprehensive national system of transportation security enhancements to protect America's maritime community against the threat of terrorism without adversely affecting the flow of commerce through United States ports. The USCG is the lead Federal agency for coordinating and implementing maritime security and has significant enforcement responsibilities under the MTSA. Among other responsibilities under MTSA, the USCG requires that maritime security plans be developed by maritime private sector industry for ports, vessels, and facilities. Additionally, the DHS/USCG—060 Homeport System of Records will be used for a limited set of individuals for the Transportation Worker Identification Credential (TWIC)

''New Hire'' Provision as delineated in USCG Navigation and Vessel Inspection Circular (NVIC) 03–07, e.h.(1). The program is for any direct hire employee who is required to have a TWIC but has not yet activated his/her card in order to allow the individual to have unaccompanied access on the facility, or vessel, for up to 30 days.

Representatives of the maritime industry entities regulated by MTSA, members of Area Maritime Security Committees (AMSC) and other officials; as well as USCG personnel will be able to register and use the DHS/USCG—060 Homeport System of Records for secure information dissemination and collaboration. Regulated entities will be able to use the DHS/USCG—060 Homeport System of Records for electronic submission and approval of required security plans, and the USCG will verify compliance with security requirements. The DHS/USCG—060 Homeport System of Records will no longer be used to collect information from and about individuals for whom background screening will be conducted for purposes of establishing USCG-approved identification credentials for access to maritime facilities. This function was terminated when the Transportation Worker Identification Credential (TWIC) requirements went into effect. Records associated with this function have been deleted. The DHS/USCG—060 Homeport System of Records will be used to collect information 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.

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, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. DHS has updated the routine uses to conform with the Department's library of routine uses. No new routine uses have been added.

II. Privacy Act

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

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/U.S. Coast Guard—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: DHS/USCG–060

SYSTEM NAME:

United States Coast Guard Homeport.

SECURITY CLASSIFICATION:

Classified, sensitive, and unclassified.

SYSTEM LOCATION:

Records are maintained at USCG Headquarters in Washington, DC and field locations including the USCG Operations Systems Center, 600 Coast Guard Drive, Kearneysville, WV 25430.

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:

Categories of records in this system include:

- 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 TWIC New Hire query, the following information will be included in accordance with 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); 33 CFR part 125.

PURPOSE(S):

The Homeport system is an enterprise tool that will facilitate 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 will allow the USCG to validate the suitablility, 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 (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 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, 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 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 on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved 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:

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 are in place to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

In accordance with AUTH: 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:

Chief, Office of Information Resources (G–PRI), U.S. 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 the USCG FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' 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* 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;
- 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;
- 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 this bulleted 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 proposed to have access to maritime facilities, government agencies, and USCG personnel.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: November 2, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–26911 Filed 11–6–09; 8:45 am]

BILLING CODE 4910–15–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–5285–N–36]

Notice of Proposed Information Collection: Comment Request, Delegated Processing for Certain 202 Supportive Housing for the Elderly Projects

AGENCY: Office of the Assistant Secretary for Housing, HUD.

ACTION: Notice.

SUMMARY: The proposed information collection requirement described below will be submitted to the Office of Management and Budget (OMB) for review, as required by the Paperwork Reduction Act. The Department is soliciting public comments on the subject proposal.

DATES: *Comments Due Date:*. January 8, 2010.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Comments should refer to the proposal by name and/or OMB Control Number and should be sent to: Lillian Deitzer, Departmental Reports Management Officer, QDAM, Department of Housing and Urban Development, 451 7th Street, SW., Washington, DC 20410; e-mail *Lillian_L._Deitzer@HUD.gov* or telephone (202) 402–8048.

FOR FURTHER INFORMATION CONTACT: Program Contact, Willie Spearmon, Director, Office of Housing Assistance and Grants Administration, Department of Housing and Urban Development, 451 7th Street, SW., Washington, DC 20410, telephone (202) 708–3000 (this is not a toll free number) for copies of the proposed forms and other available information.

SUPPLEMENTARY INFORMATION: The Department is submitting the proposed information collection to OMB for review, as required by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35, as amended).

This Notice is soliciting comments from members of the public and affected agencies concerning the proposed collection of information to: (1) Evaluate whether the proposed collection is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (2) Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information; (3) Enhance the quality, utility, and clarity of the information to be collected; and (4) Minimize the burden of the collection of information on those who are to respond; including the use of appropriate automated collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

This Notice also lists the following information:

Title of Proposal: Delegated Processing for Certain 202 Supportive Housing for the Elderly Projects

OMB Control Number, if applicable: 2502–XXXX.

Description of the need for the information and proposed use: Section 2835(b) of the Housing and Economic Recovery Act of 2008 directs the Department to delegate review and processing of certain Section 202 Supportive Housing for the Elderly projects to selected State or local housing agencies. The Delegated Processing Agreement establishes the relationship between the Department and a Delegated Processing Agency (DPA) and details the duties and compensation of the DPA. The Certifications form provides the Department with assurances that the review of the application was in accordance with HUD requirements. The Schedule of Projects form provides the DPA with information necessary to determine if they wish to process the project and upon signature commits them to such processing. Staff of the Office of Housing Assistance and Grant Administration, Multifamily Housing Office will use the information to determine if a housing finance agency wishes to participate in the program, and obtain certifications that the review of the application was in accord with HUD requirements.