In assessing the implementation of health IT, comments about the impact of particular health IT applications on different domains of a practice or clinic are requested. Thus, we would appreciate comments on how health IT has impacted or supports:

- Communication among practice or clinic staff (*e.g.,* physician, nurse, medical assistant, physician assistant, receptionist, technician).
- Coordination of care among practice or clinic staff (*e.g.,* physician, nurse, medical assistant, physician assistant, receptionist, technician).
- Information flow between the practice or clinic and external healthcare organizations (*e.g.,* community pharmacies, imaging centers, local hospitals).
- Clinicians' work during patient visit.
- Clinicians' thought processes as they care for patients.
- Access to patient-related information.

Additional Submission Instructions

Responders should identify any information that they believe is confidential commercial information. Information reasonably so labeled will be protected in accordance with the FOIA, 5 U.S.C. 552(b)(4), and will not be released by the agency in response to any FOI requests. It will not be incorporated directly into any requirements or standards that the agency may develop as a result of this inquiry regarding useful tools or information for small- and medium-sized medical practices regarding implementation of health information technology in such practices.

Dated: June 17, 2009.

Carolyn M. Clancy,

AHRQ, Director.

[FR Doc. E9–14947 Filed 6–24–09; 8:45 am]

BILLING CODE 4160–90–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2009–0082]

Homeland Security Science and Technology Advisory Committee

AGENCY: Science and Technology Directorate, DHS.

ACTION: Committee Management; Notice of Closed Federal Advisory Committee Meeting.

SUMMARY: The Homeland Security Science and Technology Advisory Committee will meet July 21–23, 2009, at Strategic Analysis, Inc. Executive Conference Center, 3601 Wilson Blvd., Suite 600, Arlington, Virginia. This meeting will be closed to the public.

DATES: The Homeland Security Science and Technology Advisory Committee will meet July 21, 2009, from 9 a.m. to 5 p.m., July 22, 2009, from 9 a.m. to 5 p.m. and on July 23, 2009, from 9 a.m. to 3 p.m.

ADDRESSES: The meeting will be held at Strategic Analysis, Inc. Executive Conference Center, 3601 Wilson Blvd., Suite 600, Arlington, Virginia. Requests to have written material distributed to each member of the committee prior to the meeting should reach the contact person at the address below by Friday, July 10, 2009. Send written material to Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528. Comments must be identified by DHS–2009–0082 and may be submitted by *one* of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *E-mail: HSSTAC@dhs.gov*. Include the docket number in the subject line of the message.
- *Fax:* 202–254–6173.
- *Mail:* Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov*, including any personal information provided.

Docket: For access to the docket to read background documents or comments received by the HSSTAC, go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528 202–254–5739.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. Annotated, Appendix 2 (Pub. L. 92–463).

At this meeting, the Committee will receive classified, SECRET-level updated threat briefings; conduct classified reviews of sensor technologies in science and technology; and receive classified reports from the Committee panels. In addition, intelligence agencies, Department of Defense and Homeland Security experts will present SECRET-level briefings concerning these matters sensitive to homeland security.

Basis for Closure: In accordance with section 10(d) of the Federal Advisory Committee Act, it has been determined that the Homeland Security Science and Technology Advisory Committee meeting concerns sensitive Homeland Security information and classified matters within the meaning of 5 U.S.C. 552b(c)(1) and (c)(9)(B) which, if prematurely disclosed, would significantly jeopardize national security and frustrate implementation of proposed agency actions and that, accordingly, the portion of the meeting that concerns these issues will be closed to the public.

Dated: June 17, 2009.

Bradley I. Buswell,

Under Secretary for Science and Technology (Acting).

[FR Doc. E9–14903 Filed 6–24–09; 8:45 am]

BILLING CODE 9110–9F–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0167]

Privacy Act of 1974; DHS/All—026 Personal Identity Verification Management System Systems of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: The Department of Homeland Security (DHS) is giving notice that it proposes to update, rename, and reissue the record system DHS/OS–2 Personal Identity Verification Management System (9/12/2006) to the DHS/All—026 Personal Identity Verification Management Record System. DHS is publishing this updated notice because the categories of individuals and categories of records have been updated, and the routine uses of this system of records notice have been updated to coincide with updates to DHS's Personal Identity Verification Management Record System. The system will support the administration of the Homeland Security Presidential Directive 12 (HSPD–12) program that directs the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems.

DATES: Written comments must be submitted on or before July 27, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0167 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: Cynthia Sjoberg, DHS HSPD–12 Program Director, Office of Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528 by telephone (202) 447–3202 or facsimile (202) 447–0119. 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), Office of Security is publishing an updated Privacy Act system of records notice to cover its collection, use and maintenance of records relating to its role in the collection and management of personally identifiable information for the purpose of issuing credentials (identification badges) to meet the requirements of the Homeland Security Presidential Directive–12 (HSPD–12) and in furtherance of the Office of Security's mission for the Department.

The Personal Identity Verification Management System (PIVMS) records will cover all DHS employees, contractors and their employees, consultants, and volunteers supporting DHS who require long-term access to Federal facilities and information systems, as well as Federal emergency response officials, foreign nationals on assignment, and other Federal employees detailed or temporarily assigned to DHS who work in Federally controlled facilities. The personally identifiable information to be collected will consist of data elements necessary to identify the individual and to perform background or other investigations concerning the individual in order to determine their suitability for access to Federal facilities. The PIVMS will collect several data elements from the personal identity verification (PIV) card applicant, including: Date of birth, Social Security Number, organizational and employee affiliations, fingerprints, digital color photograph, digital signature and phone number(s), as well as additional verification information as determined necessary. The Office of Security designed this system to align closely with its current business practices and uses set forth in this system of records notice.

DHS is publishing this updated notice to include additions to the categories of records and categories of individuals, as well as to include an additional routine use. The categories of records have been updated to include maiden name, mother's maiden name, date of birth, clearance level, identifying physical information, financial history, entry on duty date, weapons bearer designation, and an expansion on what is included in an SF–85 or equivalent form. These records are either new records in the PIV system or were erroneously excluded from the previous SORN.

The categories of individuals have expanded to include Federal emergency response officials; foreign nationals on assignment; and other Federal employees detailed or temporarily assigned to DHS, all of whom are in direct support of the DHS mission and who work in Federally controlled facilities or require access to Federal information technology systems. Lastly, DHS has added a routine use for responding to or investigating a data breach.

Consistent with DHS's information sharing mission, information stored in the PIVMS 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.

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 personally identifiable information. 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 stored and retrieved by the name of the individual or by some identifying number such as property address, mailing address, or symbol, assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. DHS extends administrative Privacy Act protections to all individuals where information is maintained on U.S. citizens, lawful permanent residents, and visitors. Individuals may request 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 5.21.

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 which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the Personal Identity Verification Management system of records.

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

System of Records:

DHS/All—026

SYSTEM NAME:

DHS/ALL Personal Identity Verification Management System (PIVMS).

SECURITY CLASSIFICATION:

Sensitive but unclassified.

SYSTEM LOCATION:

Records are maintained at Headquarters in Washington, DC, and field offices. The physical and logical access systems at all DHS and component facilities will have system-level access to the PIVMS for real-time verification of user credentials.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: All DHS employees, contractors and their employees, consultants, volunteers

engaged by DHS who require long-term access to Federally controlled facilities and information systems, as defined by Office of Management and Budget Memorandum 05–24; Federal emergency response officials; foreign nationals on assignment; and other Federal employees detailed or temporarily assigned to DHS in direct support of the DHS mission and who work in Federally controlled facilities or require access to Federal information technology systems. Individuals who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security.

The system does not apply to occasional visitors or short-term guests to whom DHS will issue temporary identification and credentials.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Full name;
- Date of birth;
- Maiden name;
- Social Security Number;
- Citizenship;
- Mother's maiden name;
- Organization/office of assignment;
- Employee affiliation and status;
- Contact information, such as telephone number(s), work e-mail, and duty location;
- Copies of identity source documents;
- Fingerprints (10 print and 2 print);
- Identifying physical information, such as height, weight, hair color, eye color, and digital photograph;
- Financial history;
- PIV card issue and expiration dates;
- PIV request form;
- PIV registrar approval digital signature;
- PIV card serial number;
- Federal emergency response official designation, affiliation, and related roles;
- Computer system user name;
- User access and permission rights, authentication certificates;
- Clearance level;
- Entry on duty date;
- Digital signature information; and
- Weapons bearer designation.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104–106, Sec. 5113); E–Government Act (Pub. L. 104–347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); and the Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504); Homeland Security Presidential Directive–12 (HSPD–12, issued August 27, 2004); Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended (40 U.S.C. 483); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, Section 3001 (50 U.S.C. 435b) and the Homeland Security Act of 2002, Pub. L. 107–296, as amended.

PURPOSE(S):

The purpose of this system is to:

- Ensure the safety and security of DHS facilities, systems, or information, and our occupants and users;
- Verify that all persons entering Federal facilities, using Federal information resources, are authorized to do so; and
- Track and control PIV cards issued to persons entering and exiting the DHS facilities or using DHS systems.

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). Disclosures may be made to:

A. To the Department of Justice (DOJ) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when:

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) 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 Department of Justice (DOJ) when:

1. The agency or any component thereof;

2. Any employee of the agency in his or her official capacity;

3. Any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or

4. The United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the

litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

I. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

J. Except as noted on Forms SF 85, 85–P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

K. To a Federal, State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.

L. To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A–19.

M. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

N. To notify another Federal agency when, or verify whether, a PIV card is no longer valid.

O. 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:

Privacy Act information may be reported to consumer reporting agencies pursuant to 5 U.S.C. 552a(b)(12).

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, paper in secure files, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by name of the individual, Social Security Number and/or by any other unique individual identifier.

SAFEGUARDS:

Records in this system are safeguarded in accordance with FISMA and other applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system 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. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary depending on the component and program.

RETENTION AND DISPOSAL:

Pursuant to GRS 18, Item 22a records used to initiate background investigations; register and enroll individuals; manage the PIV card lifecycle; and, verify, authenticate and revoke PIV cardholder access to Federal resources are destroyed upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable.

Pursuant to GRS 11, Item PIV cards are destroyed three months after they are returned to the issuing office.

Pursuant to GRS 11, Item 4a identification credentials are destroyed by cross-cut shredding no later than 90 days after deactivation.

Pursuant to GRS 18, Item 17 registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers for areas under maximum security are destroyed five years after final entry or five years after date of document, as appropriate.

Other documents pursuant to GRS 18, Item 17b are destroyed two years after final entry or two years after date of document, as appropriate.

SYSTEM MANAGER AND ADDRESS:

DHS HSPD–12 Program Director, Office of Security, U.S. Department of Homeland Security, 245 Murray Lane, SW., Building 410, Washington, DC 20528.

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 component's 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, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, 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 or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition you should provide the following:

• An explanation of why you believe the Department would have information about 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,

• 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) will 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 from the employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other Federal agencies; contract employer; former employer.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: June 18, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–14905 Filed 6–24–09; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0110]

Privacy Act of 1974; United States Coast Guard—013 Marine Information for Safety and Law Enforcement (MISLE) System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security is giving notice that it proposes to add a system of records to its inventory of record systems titled United States Coast Guard Marine Information for Safety and Law Enforcement System of Records. This system is a compilation of five legacy record systems: DOT/CG 679, Marine Information for Safety and Law Enforcement System (April 22, 2002), DOT/CG 588, Marine Safety Information System (April 11, 2000), DOT/CG 505, Recreational Boating Law Enforcement Case Files (April 11, 2000), DOT/CG 590, Vessel Identification System (April 11, 2000), DOT/CG 591, Merchant Vessel Documentation System (April 11, 2000). This record system will allow the Department of Homeland Security/United States Coast Guard to collect and maintain records regarding marine, safety and law enforcement information. Categories of individuals, categories of records, and routine uses of these legacy system of records notices have been consolidated and updated to better reflect the United States Coast Guard's marine, safety and law enforcement information. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This new system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before July 27, 2009. This new system will be effective July 27, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0110 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 and may be read at *http://www.regulations.gov,* including any personal information provided.

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

FOR FURTHER INFORMATION CONTACT: For general questions please contact: David Roberts (202–475–3521), Privacy Officer, United States Coast Guard. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (Nov. 25, 2002), the Department of Homeland Security (DHS)/United States Coast Guard (USCG) have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records regarding marine, safety and law enforcement information.

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a USCG system of records under the Privacy Act (5 U.S.C. 552a) that deals with marine safety and law enforcement information. This record system will allow DHS/USCG to collect and maintain records regarding marine safety and law enforcement information. This record system will allow the Department of Homeland Security/United States Coast Guard to collect and maintain records regarding marine information and law enforcement information.

In accordance with the Privacy Act of 1974, and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security is giving notice that it proposes to add a system of records to its inventory of record systems titled United States Coast Guard Marine Information System and Law Enforcement System of Records. This