DHS System of Records Notice Template

4410-10

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary, <Component>

DHS-2008-XXXX

Privacy Act of 1974; <Component Name> <Title of System> System of Records

AGENCY: Privacy Office; Department of Homeland Security

ACTION: Notice of Privacy Act system of records.

SUMMARY:

<Concise summary of what the system does in layman's terms. One paragraph should be enough. No abbreviations in this summary and no citations to legal authority. For legacy SORN, add legacy SORN title, Federal Register number and date issued (Month Day, Year), areas reviewed and updated (e.g. categories of individuals, categories of records, routine uses), and exemptions.>

DATES: (for new systems) The established system of records will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Written comments must be submitted on or before [insert date (30) days after publication in the Federal Register.]

ADDRESSES: You may submit comments, identified by DHS-2008-XXXX by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 1-866-466-5370.
- Mail: Hugo Teufel III, 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 go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: <component name and contact information>. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

<Provide information about why the SORN is being published. If a PIA is being conducted in conjunction with the SORN, much of this information needs to be included here.

Identify whether this is an update to a legacy system or a new system. If a legacy system, the background section must state, "Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section

1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records that concern <insert subject matter of legacy SORN.”>

Identify whether the new system is required by a new rulemaking which is being published.

Identify whether Privacy Act exemptions are being taken.

Provide the reader with a rationale for what you are doing.

Also provide a simplified discussion of the routine uses and possible examples.

Consistent with DHS’s information sharing mission, information stored in the <System Name> 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.

Last paragraph is a repeat of the summary. >

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 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 legal 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 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 "X" 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/Component-#

System name:

<Component> <SORN Title> (e.g. United States Coast Guard Motorboat Registration)

Security classification:

<Insert classification.>

System location:

Records are maintained at the <Component> Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

Categories of individuals covered by this system include: List the categories in a narrative.

Categories of records in the system:

Categories of records in this system include:

- Individual's name;
- SSN (if collected);
- Address;
- SORN specific.

Authority for maintenance of the system:

Purpose(s):

The purpose of this system is <insert brief description of the purpose>.

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 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. <Insert any additional applicable Routine Uses for specific SORNs prior to the media Routine Use below, and adjust Routine Use lettering scheme accordingly.>

I. 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:

State what information is disclosed to consumer reporting agencies. If no information is disclosed, state '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 <insert retrievability fields.>

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 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 by component and program.

Retention and disposal:

<Insert retention and disposal timeline. Reference applicable General Records Schedule (e.g. Records are maintained for 3 years in accordance with General Records Schedule X).>

System Manager and address:

<Insert System Manager and address>. Note: The System Manager does not have to be a person; a title is preferred.

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, S.W., Building 410, STOP-0550, 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 or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose form the Director, Disclosure and FOIA, 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,
- 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 by <insert sources.>

Exemptions claimed for the system:

Note any exemptions claimed for the system and the applicable regulations. If you are claiming an exemption then you will need a Notice of Proposed Rulemaking pursuant to 5 USC 552(a) outlining the reasons you are doing so. If no exemptions, state, 'None.'

Hugo Teufel III,

Chief Privacy Officer,

Department of Homeland Security.