Environmental Protection Agency. An updated listing of Federal agencies that have published LEP Guidance can be found at http://www.lep.gov/. The DOJ Recipient LEP Guidance in particular provides many helpful examples of how to apply the four-factor analysis when making decisions about the need for translating documents, obtaining interpreter, and hiring bilingual staff. See 67 FR 41466 (June 18, 2002).

Recipients may also benefit from learning about the enforcement actions of several agencies since the DOJ Guidance was first issued in 2002. For example, DOJ has entered into several agreements that are available online at http://www.lep.gov. In addition, HHS has resolved several LEP enforcement actions against health service providers. Those resolution agreements are available at http://www.hhs.gov/ocr/civilrights/activities/examples/LEP/index.html. In any compliance and enforcement activity, DHS will review the facts and circumstances pertaining to the recipient to determine whether the recipient has complied with its obligations under this guidance.

Area-specific guidance and LEP planning tools for a number of types of recipients, including municipal governments, law enforcement agencies, and recipients engaged in emergency preparedness can be found at http://www.lep.gov/resources/resources.html. Recipients are encouraged to avail themselves of these resources. In addition, the Office for Civil Rights and Civil Liberties is available to provide technical assistance to recipients on the provision of language services to LEP persons served or encountered in a recipient’s program.

As explained in this guidance, all recipients of Federal financial assistance from DHS must meet the obligation to take reasonable steps to ensure access to programs and activities by LEP persons. This guidance clarifies the Title VI regulatory obligation to address the language needs of LEP persons, in appropriate circumstances and in a reasonable manner by applying the four-factor analysis. In the context of emergency planning and response, health and safety, and law enforcement operations, where the potential for greater consequences are at issue, DHS will look for strong evidence that recipients have taken reasonable steps to ensure access.

Margo Schlanger,
Officer for Civil Rights and Civil Liberties.

[FR Doc. 2011–9336 Filed 4–15–11; 8:45 am]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Privacy Act of 1974; Consolidation of System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice to consolidate one Privacy Act system of records notice.


DATES: Effective Date: May 18, 2011.

FOR FURTHER INFORMATION CONTACT: Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235–0780 or facsimile 1–866–466–5370.

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, and as part of its ongoing integration and management efforts, the Department of Homeland Security (DHS) is giving notice that it proposes to consolidate one Privacy Act system of records notice (SORN) from its inventory of record systems titled, DHS/Directorate of Science and Technology (S&T)—0001 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, (68 FR 55642, September 26, 2003), into the existing DHS SORN titled, DHS/ALL—002 Mailing and Other Lists System, (73 FR 71659, November 25, 2008).

DHS originally created the DHS/S&T—0001 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 SORN in September 2003. This system was originally established in order to maintain records on individuals who submit applications for technologies seeking liability protection under provisions of the Support Anti-Terrorism by Fostering Effective Technologies Act. Given that these records are limited to contact information of individuals (business phone number, mailing address, e-mail address), DHS has determined this system can be covered under the DHS/ALL—002 Mailing and Other List Systems SORN.

Consolidating this SORN will have no adverse impact on individuals, but will promote the overall streamlining and management of DHS Privacy Act record systems.

Dated: April 12, 2011.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–9330 Filed 4–15–11; 8:45 am]
immunization status and general occupational health and safety, allowing them to work with specific material and use certain personal protective equipment in designated laboratory areas.

Occupational health surveillance programs are typically in place at institutions conducting biological research involving potentially high-risk agents to ensure occupational health of all personnel. As such, occupational health surveillance for contractors is commonly practiced at the S&T Laboratories and FFRDCs to ensure the health and safety of these individuals. A portion of the research conducted at the S&T Laboratories and FFRDCs involve working with biological threats and select agents and toxins. During such research, there is always a possibility that DHS contractors could become exposed to hazardous materials. It is part of biological laboratory best practices to maintain contractor’s occupational health and immunization records to ensure that appropriate and timely medical care is provided in the case of any potential risk of exposure. In the event of individual exposure, maintenance of occupational health and immunization records will facilitate appropriate mitigation and treatment of the individual.

In conjunction with occupational health surveillance, during the course of research conducted at the laboratories, contractors are often required to wear certain articles of personal protective equipment, such as respirators, in order to access and work in specific areas of the laboratory. Maintaining occupational health records helps verify that the contractor meets the health requirements to use such equipment. Additionally, DHS contractors conducting foreign travel as part of their duties at DHS have to ensure that they receive all appropriate immunizations and vaccinations prior to their travels. Managing contractor immunization records will facilitate recordkeeping of this information.

The purpose of this system is to manage, quantify, monitor, and track occupational health and immunization records of contractors working at S&T Laboratories or FFRDCs, and employees and contractors from other Federal agencies assigned to those S&T entities created in support of S&T research mission and occupational health surveillance operations. The Department’s authority for this collection is 6 U.S.C. 321e which authorizes the DHS Chief Medical Officer to ensure “internal and external coordination of all medical preparedness and response activities of the Department.” The Chief Medical Officer serves as the Department’s primary point of contact on medical and health issues, and performs such other duties relating to the Chief Medical Officer’s responsibilities as the Secretary may require. DHS Delegation 5001 (to the Assistant Secretary for Health Affairs (ASHA) and Chief Medical Officer) builds upon the Chief Medical Officer’s statutory authority in 6 U.S.C. 321e by granting the Chief Medical Officer “the authority to exercise oversight over all medical and public health activities of DHS. Section II, DHS Delegation 5001.

This system collects occupational health and immunization management records as part of S&T’s Laboratories and FFRDC occupational health surveillance operations. Efforts have been made to safeguard records in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize 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. Routine uses contained in this notice include some from the Department’s library of routine uses. Those include sharing with the Department of Justice (DOJ) for legal advice and representation; to a congressional office at the request of an individual; to the National Archives and Records Administration (NARA) for records management; to contractors in support of their contract assignment to DHS; to an agency, organization, or individual for audit; to agencies, entities, or individuals in the event of a security or information risk or compromise; to Federal, State, local and other governmental partners to enforce and prosecute laws and regulations; and to the news media where there exists a legitimate public interest. Routine Use H. is unique to this system and is for sharing with the Department of Energy when conducting research in collaboration with DHS under an interagency agreement or Memorandum of Understanding. There is no sharing with any other agencies or medical teams. This system of records will collect information under the Paperwork Reduction Act using the following forms: OMB No. 0579–0213/ 0576, APHS Application for Registration for Possession, Use and Transfer of Select

It is important to note that neither OHA or S&T are subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy regulation. “Standards for Privacy of Individually Identifiable Health Information” (Privacy Rule), 45 CFR Parts 160 and 164. OHA/S&T do not meet the statutory definition of a covered entity under HIPAA, 42 U.S.C. 1320d–1. Because OHA/S&T are not covered entities, the restrictions proscribed by the HIPAA Privacy Rule are not applicable.

This newly established system will be included in the Department of Homeland Security’s inventory of record systems.

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 pt 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/OHA–001 Contractor Occupational Health and Immunization Records 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/OHA–001.

SYSTEM NAME:

SECURITY CLASSIFICATION:
Unclassified, sensitive, and classified.

SYSTEM LOCATION:
Records may be maintained at the Directorate of Science and Technology (S&T) Headquarters in Washington, DC at S&T Laboratories or Federally Funded Research and Development Centers (FFRDC), or by the contracted Competent Medical Authority, collecting the records on behalf of S&T.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Categories of individuals covered by this system include: S&T contractors working at S&T Laboratories (and other sites); FFRDC contractors; and contractors from other Federal agencies assigned to these S&T entities, whose occupational health and immunization records are maintained in support of the S&T’s Laboratory research mission and occupational health surveillance operations. To note, Federal employees are specifically not covered by this system because they are covered by the Office of Personnel Management OPM/ GOVT–10 Employee Medical File System Records system (June 19, 2006, 71 FR 35360).

CATEGORIES OF RECORDS IN THE SYSTEM:
Categories of records in this system include:

- Individual’s full name;
- Date of birth and age;
- Gender;
- Work email address;
- Work phone number;
- Work address;
- Organizational affiliation;
- Blood type;
- Immunization record;
- Other relevant occupational health records.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
The DHS Chief Medical Officer, under 6 U.S.C. 321e is authorized to ensure “internal and external coordination of all medical preparedness and response activities of the Department”, to serve as the Department’s primary point of contact on medical and health issues, and to perform such other duties relating to the Chief Medical Officer’s responsibilities as the Secretary may require. DHS Delegation 5001 (to the Assistant Secretary for Health Affairs (ASHA) and Chief Medical Officer) builds upon the Chief Medical Officer’s statutory authority in 6 U.S.C. 321e by granting the Chief Medical Officer “the authority to exercise oversight over all medical and public health activities of” DHS. Section II, DHS Delegation 5001. Additionally, the Delegation authorizes the Chief Medical Officer to assure an effective coordinated medical response to natural or man-made disasters or acts of terrorism, including “[s]upporting the National Operations Center, National Response Coordination Center, and Component leadership to ensure that operations have appropriate medical support, to specifically include coordination of medical activities for any level of incident with biological or medical consequences.”

PURPOSE(S):
The purpose of this system is to manage, quantify, monitor, and track occupational health and immunization records of contractors working at S&T Laboratories or FFRDCs, and employees and contractors from other Federal agencies assigned to those S&T entities created in support of S&T research mission and occupational health surveillance operations.

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;
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 2006.

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 whom the record pertains.

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, 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 Energy when conducting research in collaboration with DHS under an interagency agreement, a Memorandum of Understanding, or Memorandum of Agreement.

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:

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 an individual’s name, date of birth, e-mail address, and/or work telephone number.

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 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:

Records will be maintained in accordance with the National Archives and Records Administration (NARA) approved General Records System 1, Item 19, which covers forms, correspondence, and other records, including summary records documenting an individual employee’s medical history, physical condition, and visits to the Government health-facilities, for non-work related purposes. Occupational health and immunization records maintained at field sites will be retained by the laboratories contract operators. Records are deleted/ destroyed when S&T or laboratory contract operators determine that they are no longer needed for administrative, legal, audit, or other operational purposes.

SYSTEM MANAGER AND ADDRESS:


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 S&T’s FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under “contacts.”

When seeking records about yourself from this 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
DEPARTMENT OF HOMELAND SECURITY
Coast Guard
[Docket No. USCG–2011–0204]

Navigation Safety Advisory Council

AGENCY: Coast Guard, DHS.

ACTION: Notice of Federal Advisory Committee Meeting.

SUMMARY: The Navigation Safety Advisory Council (NAVSAC) will meet on May 4–5, 2011, in Arlington, Virginia. The meeting will be open to the public.

DATES: NAVSAC will meet Wednesday, May 4, 2011, from 8 a.m. to 5 p.m., and Thursday, May 5, 2011, from 8 a.m. to 5 p.m. Please note that the meeting may close early if the committee has completed its business. Pre-registration and written comments are due April 29, 2011.

ADDRESSES: The meeting will be held at the Navy League Building, Coast Guard Recruiting Command, 5th floor conference room, 2300 Wilson Boulevard, Suite 500, Arlington, Virginia 20598. All visitors to the Navy League Building must pre-register to be admitted to the building. You may pre-register by contacting the person listed in FOR FURTHER INFORMATION CONTACT below.

For information on facilities or services for individuals with disabilities or to request special assistance at the meeting, contact Mr. Dennis Fahr as soon as possible.

To facilitate public participation, we are inviting public comment on the issues to be considered by the committee as listed in the “Agenda” section below. You may submit written comments no later than April 25, 2011, and must be identified by USCG–2011–0204 using one of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments (preferred method to avoid delays in processing).
- Hand Delivery: Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

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. You may review a Privacy Act notice regarding our public docket in the January 17, 2008, issue of the Federal Register (73 FR 3316).

A public comment period will be held during the meeting on May 4, 2011, from 3 to 4 p.m., and May 5, at the close of the meeting. Speakers are requested to limit their comments to 10 minutes. Please note that the public comment period may end before the time indicated, following the last call for comments. Contact the individual listed below to register as a speaker.

FOR FURTHER INFORMATION CONTACT: If you have questions about this meeting, please contact Mr. Mike Sollosi, the NAVSAC Alternate Designated Federal Officer (ADFO), at telephone 202–372–1545 or e-mail mike.m.sollosi@uscg.mil, or Mr. Dennis Fahr, at telephone 202–372–1531 or e-mail dennis.fahr@uscg.mil. If you have questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826.

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

The NAVSAC is an advisory committee authorized in 33 U.S.C. 2073 and chartered under the provisions of the FACA. NAVSAC provides advice and recommendations to the Secretary, through the Commandant of the U.S. Coast Guard, on matters relating to prevention of maritime collisions, rammings, and groundings; including the Inland and International Rules of the Road, navigation regulations and equipment, routing measures, marine information, diving safety, and aids to navigation systems.

Agenda

The NAVSAC will meet to review, discuss and formulate recommendations on the following topics:

- Wednesday, May 4, 2011

  (1) Coastal Marine Spatial Planning (CMSP)

     Executive Order 13547 directed Federal Agencies to take a new approach to stewardship of the oceans, coasts, and Great Lakes. CMSP is one facet of that initiative. This topic will address the Coast Guard’s plans for implementing CMSP.

  (2) Navigation Rules Regulatory Project

     This topic will address the Coast Guard’s progress toward implementing NAVSAC approved changes to the Inland Navigation Rules.

  (3) E-Navigation Strategy

     Under the auspices of the Committee on the Marine Transportation System, the Coast Guard and other agencies are developing a National e-Navigation Strategy that will establish a framework for data exchange between and among ships and shore facilities. This topic will update the Council on that effort.

  (4) Electronic Chart Display and Information System (ECDIS)

     Mandatory carriage of ECDIS will be phased in beginning in 2012. This series of presentations will inform the Council of developments and difficulties encountered in deploying ECDIS, including accuracy of charted positions, the range of vessels to be impacted, and training requirements for ECDIS.

  (5) Virtual Aids to Navigation

     Aids to Navigation authorities are considering deploying virtual aids to navigation as an alternative to physical lights, daybeacons and buoys under certain circumstances. This topic will inform the Council on virtual aids and discuss their possible use in U.S. waters.