DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Eye Institute; Notice of Closed Meetings

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meetings. The meetings will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Eye Institute Special Emphasis Panel, NEI Research Program Grant Applications II.

Date: July 6, 2011.

Time: 1:30 p.m. to 2:30 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, NEI, 5635 Fishers Lane, Rockville, MD 20892, (Telephone Conference Call).

Contact Person: Anne E. Schaffner, PhD, Scientific Review Officer, Division of Extramural Research, National Eye Institute, National Institutes of Health, 5635 Fishers Lane, Suite 1300, MSC 9300, 301–451–2020, aes@nei.nih.gov.

This notice is being published less than 15 days prior to the meeting due to the timing limitations imposed by the review and funding cycle.

Name of Committee: National Eye Institute Special Emphasis Panel, NEI Mentored Training Grant Applications.

Date: July 18–19, 2011.

Time: 9 a.m. to 9 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, NEI, 5635 Fishers Lane, Rockville, MD 20892, (Virtual Meeting).

Contact Person: Anne E. Schaffner, PhD, Scientific Review Officer, Division of Extramural Research, National Eye Institute, National Institutes of Health, 5635 Fishers Lane, Suite 1300, MSC 9300, 301–451–2020, aes@nei.nih.gov.

The meeting will be open to the public as indicated below, with attendance limited to space available. Individuals who plan to attend and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Advisory Council on Alcohol Abuse and Alcoholism.

Date: September 12–13, 2011.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute on Alcohol Abuse and Alcoholism; Notice of Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of a meeting of the National Advisory Council on Alcohol Abuse and Alcoholism.

The meeting will be open to the public as indicated below, with attendance limited to space available. Individuals who plan to attend and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Advisory Council on Alcohol Abuse and Alcoholism.

Date: September 12–13, 2011.

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2011–0052]

DHS Data Privacy and Integrity Advisory Committee

AGENCY: Privacy Office, DHS.

ACTION: Committee Management; Request for Applicants for Appointment to the DHS Data Privacy and Integrity Advisory Committee.

SUMMARY: The Department of Homeland Security Privacy Office is seeking applicants for appointment to the DHS Data Privacy and Integrity Advisory Committee.

DATES: Applications for membership must reach the Department of Homeland Security Privacy Office at the address below on or before August 15, 2011.

ADDRESSES: If you wish to apply for membership, please submit the documents described below to Martha K. Landesberg, Executive Director, DHS.
Data Privacy and Integrity Advisory Committee, by either of the following methods:

- E-mail: PrivacyCommittee@dhs.gov. Include the Docket Number (DHS–2011–0052) in the subject line of the message.
- Fax: (703) 235–0442.

FOR FURTHER INFORMATION CONTACT:
Martha K. Landesberg, Executive Director, DHS Data Privacy and Integrity Advisory Committee, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235–0780, by fax (703) 235–0442, or by e-mail to PrivacyCommittee@dhs.gov.

SUPPLEMENTARY INFORMATION: The DHS Data Privacy and Integrity Advisory Committee is an advisory committee established in accordance with the provisions of the Federal Advisory Committee Act (FACA), 5 U.S.C.A. App. 2. The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. 451 and provides advice at the request of the Secretary and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information (PII), as well as data integrity and other privacy-related matters. The duties of the Committee are solely advisory in nature. In developing its advice and recommendations, the Committee may, consistent with the requirements of the FACA, conduct studies, inquiries, workshops and seminars in consultation with individuals and groups in the privacy sector and/or other governmental entities. The Committee typically meets four times in a calendar year.

Committee Membership: The DHS Privacy Office is seeking applicants for terms to expire on January 31, 2014. Members are appointed by and serve at the pleasure of the Secretary of the Department of Homeland Security, and must be specially qualified to serve on the Committee by virtue of their education, training, and experience in the fields of data protection, privacy, and/or emerging technologies. Pursuant to the FACA, the Committee’s Charter requires that Committee membership be balanced to include:

1. Individuals who are currently working in the areas of higher education or research in public (except Federal) or not-for-profit institutions;
2. Individuals currently working in non-governmental industry or commercial interests, including at least one individual who is familiar with the data concerns of small to medium enterprises; and
3. Other individuals, as determined appropriate by the Secretary.

Committee members serve as Special Government Employees (SGE) as defined in section 202(a) of title 18 United States Code. As such, they are subject to Federal conflict of interest laws and government-wide standards of conduct regulations. Members must annually file Confidential Financial Disclosure Reports (OGE Form 450) for review and approval by Department ethics officials. DHS may not release these reports or the information in them to the public except under an order issued by a Federal court or as otherwise provided under the Privacy Act (5 U.S.C. 552a). Committee members are also required to have an appropriate security clearance as a condition of their appointment.

Members are not compensated for their service on the Committee; however, while attending meetings or otherwise engaged in Committee business, members may receive travel expenses and per diem in accordance with Federal regulations.

Committee History and Activities: All individuals interested in applying for Committee membership should review the history of the Committee’s work. The Committee’s charter and current membership, transcripts of Committee meetings, and all of the Committee’s reports and recommendations to the Department are posted on the Committee’s Web page on the DHS Privacy Office Web site (http://www.dhs.gov/privacy).

Applying for Membership
If you are interested in applying for membership on the DHS Data Privacy and Integrity Advisory Committee, please submit the following documents to Martha K. Landesberg, Executive Director, at the address provided below by August 15, 2011:

1. A current resume; and
2. A letter that explains your qualifications for service on the Committee and describes in detail how your experience is relevant to the Committee’s work.

Your resume and your letter will be weighed equally in the application review process. Please note that by Administration policy individuals who are registered as Federal lobbyists are not eligible to serve on Federal advisory committees. If you are registered as a Federal lobbyist and you have actively lobbied at any time since August 15, 2009, you are not eligible to apply for membership on the DHS Data Integrity Advisory Committee. Applicants selected for membership will be required to certify, pursuant to 28 U.S.C. 1746, that they are not registered as Federal lobbyists. Please send your documents to Martha K. Landesberg, Executive Director, DHS Privacy and Integrity Advisory Committee, by either of the following methods:

- E-mail: PrivacyCommittee@dhs.gov.
- Fax: (703) 235–0442.

Privacy Act Statement: DHS's Use of Your Information


Principal Purposes: When you apply for appointment to the DHS Data Privacy and Integrity Advisory Committee, DHS collects your name, contact information, and any other personal information that you submit in conjunction with your application. We will use this information to evaluate your candidacy for Committee membership. If you are chosen to serve as a Committee member, your name will appear in publicly-available Committee documents, membership lists, and Committee reports.

Routine Uses and Sharing: In general, DHS will not use the information you provide for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or as necessary for a specific purpose, as described in the DHS/ALL–009 Department of Homeland Security Advisory Committees System of Records Notice (October 3, 2008, 73 FR 63181).

Effects of Not Providing Information: You may choose not to provide the requested information or to provide only some of the information DHS requests. If you choose not to provide some or all of the requested information, DHS may not be able to consider your application for appointment to the Data Privacy and Integrity Advisory Committee.

Accessing and Correcting Information: If you are unable to access or correct this information by using the method that you originally used to submit it, you may direct your request in writing to the DHS Chief FOIA Officer at foia@dhs.gov. Additional instructions are available at http://www.dhs.gov/foia and in the DHS/ALL–002 Mailing and Other Lists System of Records referenced above.
Dated: June 29, 2011.

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

[FR Doc. 2011–18604 Filed 7–5–11; 8:45 am]

BILLING CODE 9110–9L–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2011–0061]

Privacy Act of 1974; Department of Homeland Security/ALL–030 Use of the Terrorist Screening Database System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.


Homeland Security Presidential Directive 6 (HSPD–6), issued in September 2003, called for the establishment and use of a single consolidated watchlist to improve the identification, screening, and tracking of known or suspected terrorists and their supporters. The FBI/TSC maintains and distributes the TSDB as the U.S. government’s consolidated terrorist watchlist. DHS and the FBI/TSC, working together, have developed the DHS Watchlist Service (WLS) in order to automate and simplify the current method for transmitting TSDB records from the FBI/TSC to DHS and its components.

The WLS allows the FBI/TSC and DHS to move away from a manual and cumbersome process of data transmission and management to an automated and centralized process. The WLS will replace multiple data feeds from the FBI/TSC to DHS and its components, as documented by information sharing agreements, with a single feed from the FBI/TSC to DHS and its components. The WLS is a system to system secure connection with no direct user interface.

DHS and its components are authorized to access TSDB records via the WLS pursuant to the terms of information sharing agreements with FBI/TSC. DHS is publishing this SORN and has published privacy impact assessments to provide additional transparency into how DHS has implemented WLS. DHS will review and update this SORN no less than biennially as new DHS systems come online with the WLS and are approved consistent with the terms of agreements with FBI/TSC. There are five DHS systems that currently receive TSDB data directly from the FBI/TSC and will use the WLS. These systems have existing SORNs that cover the use of the TSDB:

(1) Transportation Security Administration (TSA), Office of Transportation Threat Assessment and Credentialing: DHS/TSA–002 Transportation Security Threat Assessment System (May 19, 2010, 75 FR 28046);

(2) TSA, Secure Flight Program: DHS/TSA–019 Secure Flight Records System (November 9, 2007, 72 FR 63711);

(3) U.S. Customs and Border Protection (CBP), Passenger Systems Program Office for inclusion in TECS: DHS/CBP–011 TECS System (December 19, 2008 73 FR 77778);

(4) U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT), Program for inclusion into the DHS Enterprise Biometrics Service (IDENT) DHS/USVISIT–0012 DHS Automated Biometric Identification System (June 5, 2007, 72 FR 31080); and

In addition, two DHS components will receive TSDB data via the WLS in the form of a computer readable extract. The components’ use of the TSDB data is covered by existing SORNs:

(1) Office of Intelligence and Analysis (I&A): DHS/IA–001 Enterprise Records System, (May 15, 2008 73 FR 28128), and


Information stored in the WLS will be shared back with the FBI/TSC in order to ensure that DHS and the FBI/TSC can reconcile any differences in the database and ensure DHS has the most up-to-date and accurate version of TSDB records. All other sharing will be conducted pursuant to the programmatic system of records notices and privacy impact assessments discussed in this SORN.

DHS is planning future enhancements to the WLS that will provide for a central mechanism to receive information from DHS components when they encounter a potential match to the TSDB and send this information to the FBI/TSC. DHS will update this SORN to reflect such enhancements to the WLS, as part of its biennial reviews of this SORN once that capability is implemented.

DHS is publishing this SORN to cover the Department’s use of the TSDB in