

of operation. This measured expansion of biometrics at sea will assist in the prosecution of persons engaged in such activities as illegal maritime migration, smuggling, illegal drug transportation, and other types illegal maritime activity. By deterring unsafe and illegal maritime migration and other illegal activities at sea, the use of biometrics will promote an important USCG mission, in particular the preservation of life at sea and the enforcement of U.S. law.

*System:* Western Hemisphere Travel Initiative Land and Sea Final Rule.

*Component:* Customs and Border Protection.

*Date of approval:* March 24, 2008.

DHS and CBP, in conjunction with the Bureau of Consular Affairs at the Department of State, published in the **Federal Register** a final rule to notify the public of how they will implement the Western Hemisphere Travel Initiative (WHTI) for sea and land ports of entry. The final rule removes the current regulatory exceptions to the passport requirement provided under sections 212(d)(4)(B) and 215(b) of the Immigration and Nationality Act. On August 9, 2007, the DHS Privacy Office issued a PIA for the proposed rule, which was published in the **Federal Register** on June 26, 2007, at 72 FR 35088. This PIA updates the earlier PIA for the proposed rule to reflect changes in the WHTI final rule for land and sea ports-of-entry.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-16044 Filed 7-14-08; 8:45 am]

BILLING CODE 4410-10-P

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

#### Published Privacy Impact Assessments on the Web

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Publication of Privacy Impact Assessments.

**SUMMARY:** The Privacy Office of the Department of Homeland Security (DHS) is making available ten (10) Privacy Impact Assessments on various programs and systems in the Department. These assessments were approved and published on the Privacy Office's Web site between October 1, 2007, and December 31, 2007.

**DATES:** The Privacy Impact Assessments will be available on the DHS Web site until September 15, 2008, after which they may be obtained by contacting the

DHS Privacy Office (contact information below).

**FOR FURTHER INFORMATION CONTACT:**

Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Mail Stop 0550, Washington, DC 20528, or e-mail: [pia@dhs.gov](mailto:pia@dhs.gov).

**SUPPLEMENTARY INFORMATION:** Between October 1 and December 31, 2007, the Chief Privacy Officer of the Department of Homeland Security (DHS) approved and published ten (10) Privacy Impact Assessments (PIAs) on the DHS Privacy Office Web site, <http://www.dhs.gov/privacy>, under the link for "Privacy Impact Assessments." These PIAs cover ten (10) separate DHS programs. Below is a short summary of those programs, indicating the DHS component responsible for the system, and the date on which the PIA was approved. Additional information can be found on the Web site or by contacting the Privacy Office.

*System:* Transportation Worker Identification Credential Program Final Rule.

*Component:* Transportation Security Administration.

*Date of approval:* October 5, 2007.

The Transportation Security Administration (TSA) published a joint Final Rule with the United States Coast Guard to implement a Transportation Worker Identification Credential (TWIC) program to provide a biometric credential that can be used to confirm the identity of workers in the national transportation system, and conducted a PIA associated with that Final Rule. TSA is amending the PIA to reflect the development of TWIC contactless card capability in sections 1.4, 1.6, 9.2 and 9.3, and the approval of the records schedule by NARA in section 3. This PIA replaces the one published December 29, 2006.

*System:* Universal Commercial Driver's License (CDL) Security Threat Assessment.

*Component:* Transportation Security Administration.

*Date of approval:* October 12, 2007.

TSA conducts security threat assessments on Commercial Driver's License (CDL) holders. CDL holders are licensed to operate large commercial motor vehicles that potentially pose threats to transportation security. Congress directed TSA to perform threat assessments on certain CDL holders in the SAFE PORT Act Pub. L. No. 109-347, 120 Stat. 1884 (2006). Since the potential threat extends beyond ports, TSA will perform security threat assessments on all CDL holders pursuant to its authority under 49 U.S.C. 14(f) which gives TSA broad

authority "to assess threats to transportation" including vetting persons who could pose a threat to transportation.

*System:* Visitor Management System.

*Component:* Transportation Security Administration.

*Date of approval:* October 19, 2007.

The PIA previously published on July 14, 2006, has been amended to reflect the collection of a photograph to be placed on the temporary badge. The photograph will be stored in the system only for so long as is required to create the badge, then is deleted to create the next badge. This PIA replaces the previously published PIA.

*System:* Airmen Certificate Vetting Program.

*Component:* Transportation Security Administration.

*Date of approval:* October 22, 2007.

TSA implemented a process to conduct security threat assessments on all Federal Aviation Administration (FAA) Airmen Certificate applicants and holders to ensure that the individual does not pose or is not suspected of posing a threat to transportation or national security. FAA Airmen Certificate holders include pilots, air crews, and others required to hold a certificate pursuant to FAA regulations. Because this program entails a new collection of information by TSA about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 require that the TSA issue a PIA. The data collected and maintained for this program and the details and uses of this information are outlined in this PIA.

*System:* DHS/UKvisas Project.

*Component:* U.S. Citizenship and Immigration Services.

*Date of approval:* November 14, 2007.

Recently the United Kingdom (UK) enacted legislation requiring the submission of biometric data by almost all individuals filing applications for UK visas. Officials from the UK and DHS have agreed that individuals who are physically located in the United States (US) may provide the requisite biometrics and limited biographical information at U.S. Citizenship and Immigration Services (USCIS) Application Support Centers (ASCs) for forward transfer to the UK in support of the adjudication of applications for visas. USCIS will temporarily retain the submitted biometric and biographical records until the UK provides confirmation that the transfer of data was successful. USCIS will delete the biometric and biographical records immediately after it receives that confirmation.

*System:* Conversion to 10-Fingerprint Collection for the United States Visitor and Immigrant Status Indicator Technology Program.

*Component:* US-VISIT.

*Date of approval:* November 15, 2007.

US-VISIT is an office and program within the National Protection and Programs Directorate of DHS. The office manages DHS' IDENT system and provides biometrics-based identity management services to agencies throughout immigration and border management, law enforcement, and intelligence communities. The Program provides an integrated, automated, biometric entry and exit system that records the arrival and departure of foreign nationals. US-VISIT published this PIA to update and describe the US-VISIT Program's change from collecting two (2) fingerprints to collecting up to ten (10) fingerprints (using inkless optical reading devices) from foreign nationals upon entering or exiting the United States.

*System:* National Infrastructure Coordinating Center INSight Application.

*Component:* National Protection and Programs Directorate.

*Date of approval:* November 23, 2007.

The National Infrastructure Coordinating Center (hereafter refer to as the NICC), part of the National Operations Center (NOC) in the Operations Directorate, operates the INSight Information Management System (INSight), designed to support the identification of potentially significant changes in the operational status of the nation's Critical Infrastructures and Key Resources so that trained analysts can provide timely coordination with the NOC, respective Information Sharing and Analysis Centers, and other involved agencies in the public sector and federal sectors. INSight may collect personally identifiable information (PII) associated with infrastructure information; accordingly NICC has conducted this PIA.

*System:* Boarding Pass Scanning System.

*Component:* Transportation Security Administration.

*Date of approval:* November 29, 2007.

The Boarding Pass Scanning System (BPSS) is a process and technology that validates the authenticity of the boarding pass at the TSA security checkpoint using 2-dimensional (2D) bar code readers and encryption techniques. The BPSS will display machine readable data from the boarding pass for confirmation against the human readable portions of the boarding pass to verify that the boarding

pass is legitimate and has not been tampered with. Once confirmed, the displayed data will be deleted from the BPSS.

*System:* Enterprise Correspondence Tracking System (ECT).

*Component:* Department Wide.

*Date of approval:* December 3, 2007.

The Executive Secretariat of DHS operates the Enterprise Correspondence Tracking (ECT) system. The ECT is a correspondence workflow management system that assists DHS in responding to inquiries from the public, other government agencies, and the private sector. Tens of thousands of pieces of correspondence ranging from official rulings, policy statements, testimony, or even thank you letters are processed annually by DHS. The Executive Secretariat conducted this privacy impact assessment because the ECT collects and uses PII.

*System:* DHSAccessGate System.

*Component:* Management.

*Date of approval:* December 3, 2007.

DHS added a new layer of security to its vendor employee access control procedures at certain facilities by offering a new and voluntary vendor program called the DHSAccessGate Program. Part of this program will involve the collection of PII from individuals who are not DHS employees or contractors. The DHS Office of Security has conducted this privacy impact assessment because of the collection of new PII.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-16045 Filed 7-14-08; 8:45 am]

**BILLING CODE 4410-10-P**

## DEPARTMENT OF HOMELAND SECURITY

### Federal Emergency Management Agency

[Docket ID: FEMA-2007-0008]

#### National Advisory Council Meeting

**AGENCY:** Federal Emergency Management Agency, DHS.

**ACTION:** Notice of Federal Advisory Committee Meeting.

**SUMMARY:** This notice announces the date, time, location, and agenda for the next meeting of the National Advisory Council (NAC). At the meeting, the subcommittees will be reporting back regarding their work since the May 14-15, 2008 meeting. This meeting will be open to the public.

**DATES:** *Meeting Dates:* Wednesday, August 13, 2008, from approximately 11

a.m. to 5 p.m. and Thursday, August 14, 2008, 9 a.m. to 4:30 p.m. A public comment period will take place on the afternoon of August 14, 2008, between approximately 2:30 p.m. and 3 p.m.

*Comment Date:* Written comments or requests to make oral presentations must be received by August 6, 2008.

**ADDRESSES:** The meeting will be held at the Grand Hyatt Washington, 1000 H St. NW., Washington, DC 20001. Persons wishing to make an oral presentation, or who are unable to attend or speak at the meeting, may submit written comments. Written comments and requests to make oral presentations at the meeting should be provided to the address listed in the

**FOR FURTHER INFORMATION CONTACT** section and must be received by August 6, 2008. All submissions received must include the Docket ID FEMA-2007-0008 and may be submitted by any one of the following methods:

*Federal Rulemaking Portal:* <http://www.regulations.gov>. Follow instructions for submitting comments on the Web site.

*E-mail:* [FEMA-RULES@dhs.gov](mailto:FEMA-RULES@dhs.gov). Include Docket ID FEMA-2007-0008 in the subject line of the message.

*Facsimile:* (866) 466-5370.

*Mail:* Office of Chief Counsel, Federal Emergency Management Agency, Room 835, 500 C Street, SW., Washington, DC 20472.

*Hand Delivery/Courier:* Office of the Chief Counsel, Federal Emergency Management Agency, Room 835, 500 C Street, SW., Washington, DC 20472.

*Instructions:* All submissions received must include the Docket ID FEMA-2007-0008. Comments received will also 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 National Advisory Council, go to <http://www.regulations.gov>.

#### FOR FURTHER INFORMATION CONTACT:

Alyson Price, Designated Federal Officer, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472, telephone 202-646-3746, fax 202-646-3061, and e-mail [FEMA-NAC@dhs.gov](mailto:FEMA-NAC@dhs.gov) or

[Jennifer.Veal@associates.dhs.gov](mailto:Jennifer.Veal@associates.dhs.gov). The NAC's Web site is located at: <http://www.fema.gov/about/nac/>.

**SUPPLEMENTARY INFORMATION:** Notice of this meeting is given under the Federal Advisory Committee Act (FACA), Public Law 92-463, as amended (5 U.S.C. App. 1 *et seq.*). The National Advisory Council (NAC) will meet for the purpose of reviewing the progress of the NAC subcommittees, to receive an update on