Dated: July 9, 2008.

John Campbell,

Acting Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. E8–16166 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 sixteen (16) 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 January 1 and March 31, 2008.

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*.

SUPPLEMENTARY INFORMATION: Between January 1 and March 31, 2008, the Chief Privacy Officer of the Department of Homeland Security (DHS) approved and published sixteen (16) 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 sixteen (16) 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: Whole Body Imaging.

Component: Transportation Security Administration.

Date of approval: January 2, 2008.

The Transportation Security Administration (TSA) is conducting pilot operations to evaluate the use of various Whole Body Imaging (WBI) technologies, including backscatter x-ray and millimeter wave devices, to detect threat objects carried on persons entering airport sterile areas. WBI creates an image of the full body, showing the surface of the skin and revealing objects that are on the body, not in the body. To mitigate the privacy risk associated with creating an image of the individual's body, TSA isolates the Transportation Security Officer (TSO) viewing the image from the TSO interacting with the individual. During the initial phase of the pilot, individuals who must undergo secondary screening will be given the option of undergoing the normal secondary screening technique involving a physical pat down by a TSO or a screening by a WBI device. A subsequent phase will evaluate WBI technology for individuals undergoing primary screening. Individuals will be able to choose to undergo WBI screening in primary.

System: Federal Flight Deck Officer Program.

Component: Transportation Security Administration.

Date of approval: January 10, 2008.

The Federal Flight Deck Officer program was established by the Arming Pilots Against Terrorism Act as Title XIV of the Homeland Security Act (Pub. L. 107–296, Nov. 25, 2003, 116 Stat. 2300), codified at 49 U.S.C. 44921. Under this program, TSA deputizes qualified volunteer pilots and flight crewmembers of passenger and cargo aircraft as law enforcement officers to defend the flight deck of aircraft against acts of criminal violence or air piracy. Participants in the program, known as Federal Flight Deck Officers (FFDOs), are trained and authorized to transport and carry a firearm and to use force, including deadly force. Through this program, TSA collects data on pilots to assess the qualification and suitability of prospective and current FFDOs through an online application, and to administer the program.

System: The Department of Homeland Security REAL–ID Final Rule.

Component: DHS-Wide.

Date of approval: January 11, 2008.

DHS issued a final rule establishing minimum standards for State-issued driver's licenses and identification cards that Federal agencies will accept for official purposes after May 11, 2008, in accordance with the REAL–ID Act of 2005, Pub. L. 109–13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note) (the Act). The final rule establishes standards to meet the minimum requirements of the Act including: Information and security features that must be incorporated into each card; application information to establish the identity and lawful status of an applicant before a card can be issued; and physical security standards for locations issuing driver's licenses and identification cards.

System: Personnel Security Activities Management System/Integrated Security Management System Update.

Component: DHS-Wide.

Date of approval: January 15, 2008.

The DHS Office of Security uses the Integrated Security Management System (ISMS) to automate the tracking of Personnel Security related activities at DHS headquarters and component sites. ISMS is an update system to the Personnel Security Activities Management System (PSAMS). ISMS will help manage DHS personnel and security case records by adding to the existing functionality of PSAMS.

System: USCIS Person Centric Query Service Supporting the Verification Information System.

Component: U.S. Citizenship and Immigration Services.

Date of approval: January 18, 2008.

This is an update to the PIA for the USCIS Person Centric Query (PCQ) Service, operating through the USCIS Enterprise Service Bus (ESB) to describe the privacy impact of expanding the PCQ Service to include the following additional PCQ Client: The National Security and Records Verification Directorate/Verification Division's VIS.

System: USCIS Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS National Security and Records Verification Directorate/Verification Division.

Component: U.S. Citizenship and Immigration Services.

Date of approval: January 18, 2008.

This is an update to the PIA for the USCIS PCQ Service, operating through the USCIS ESB to describe the privacy impact of expanding the PCQ Service to include the following additional PCQ Client: The Immigrant Status Verifiers of the USCIS National Security and Records Verification Directorate/Verification Division.

System: Use of Radio Frequency Identification (RFID) Technology for Border Crossings.

Component: Customs and Border Protection.

Date of approval: January 22, 2008.

U.S. Customs and Border Protection (CBP) employs Radio Frequency Identification (RFID) Technology that is to be used in cross-border travel documents to facilitate the land border primary inspection process. A unique number is embedded in an RFID tag which, in turn, is embedded in each cross-border travel document. At the border, the unique number is read wirelessly by CBP and then forwarded through a secured data circuit to back-end computer systems. The back-end

systems use the unique number to retrieve personally identifiable information (PII) about the traveler. This information is sent to the CBP Officer to assist in the authentication of the identity of the traveler and to facilitate the land border primary inspection process. Multiple border crossing programs use or plan to take advantage of CBP's vicinity RFID-reader enabled border crossing functionality including CBP's own trusted traveler programs, the pending Department of State's Passport Card, the Mexican Border Crossing Card, the proposed Enhanced Driver's License offered by various states, tribal enrollment cards that could be developed by various Native American Tribes, and the proposed Enhanced Driver's Licenses being developed within the various provincial authorities in Canada.

System: ICE Pattern Analysis and Information Collection (ICEPIC).

Component: Immigration and Customs Enforcement.

Date of approval: January 30, 2008.

U.S. Immigration and Customs Enforcement (ICE) has established a system called the ICE Pattern Analysis and Information Collection (ICEPIC) system. ICEPIC is a toolset that assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. All ICEPIC activity is predicated on ongoing law enforcement investigations. This PIA is being completed to provide additional notice of the existence of the ICEPIC system and publicly document the privacy protections that are in place for the ICEPIC system.

System: Office of Inspector General Investigative Records.

Component: Office of Inspector General.

Date of approval: January 30, 2008.

DHS Office of Inspector General (OIG) Investigative Records System includes both paper investigative files and the ''Investigations Data Management System'' (IDMS)—an electronic case management and tracking information system, which also generates reports. OIG uses IDMS to manage information relating to DHS OIG investigations of alleged criminal, civil, or administrative violations relating to DHS employees, contractors and other individuals and entities associated with the DHS. This PIA is being conducted to assess the privacy impact of the OIG Investigative Records system that includes both paper investigative files and the IDMS.

System: Crew Member Self Defense Training (CMSDT) Program.

Component: Transportation Security Administration.

Date of approval: February 6, 2008.

DHS TSA has developed the Crew Member Self-Defense Training Program (CMSDT), a voluntary self-defense training course, for air carrier crew members. TSA will collect name, last four (4) numerals of the Social Security Number, contact information, employer information including employee identification number, and course location preferences in order to verify a crew member's eligibility for the program and to provide the self-defense training. Because the CMSDT collects PII on members of the public, TSA is conducting this PIA in accordance with the statutory requirements of the E-Government Act of 2002.

System: Science and Technology's Experimental Testing of Project Hostile Intent Technology.

Component: Science and Technology.

Date of approval: February 25, 2008.

Project Hostile Intent (PHI) is a research effort by the Science and Technology Directorate to ascertain whether screening technology can aid DHS screeners in making better decisions by supplementing the current screening process (wherein a human screener evaluates an individual's behavior) with training and computers. This PIA addresses privacy impacts of this program, and specifically, the temporary storage of video images during field tests of PHI's performance with real behavioral data to ensure that it is effective in a ''real world'' environment.

System: Protected Repository for the Defense of Infrastructure Against Cyber Threats.

Component: Science and Technology.

Date of approval: February 25, 2008.

The Science & Technology Directorate's Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) system is a repository of test datasets of Internet traffic data that is made available to approved researchers and managed by an outside contractor serving as the PREDICT Coordination Center. The goal of PREDICT is to create a national research and development resource to bridge the gap between (a) the producers of security-relevant network operations data and (b) technology developers and evaluators who can use this data to accelerate the design, production, and evaluation of next-generation cyber security solutions, including commercial products. A key motivation of PREDICT is to make these data sources more widely available to technology developers and evaluators, who are currently forced to base the efficacy of their technical solutions on old, irrelevant traffic data, anecdotal evidence, or small-scale test experiments, rather than on more comprehensive, real-world data analysis.

System: USCIS Verification Information System Supporting Verification Programs.

Component: U.S. Citizenship and Immigration Services.

Date of approval: February 28, 2008.

The Verification Division of the U.S. Citizenship and Immigration Services (USCIS) operates the Verification Information System (VIS). VIS is a composite information system incorporating data from various DHS databases. It is the underlying information technology that provides immigration status verification for (1) benefits determinations through the Systematic Alien Verification for Entitlements (SAVE) program for government benefits and (2) verification of employment authorization for newly hired employees through the E-Verify program. USCIS is conducting this PIA to clarify previous VIS PIAs and to describe updates to VIS that will improve the ability of USCIS to verify citizenship and immigration status information to users of SAVE and E-Verify.

System: DHS Enterprise e-Recruitment System.

Component: DHS Wide.

Date of approval: March 4, 2008.

Office of the Chief Human Capital Officer (OCHCO) implemented an enterprise e-Recruitment system for DHS. The use of an automated recruitment solution is necessary to meet mission critical needs of DHS and comply with the 45-day hiring model under the President's Management Agenda. OCHCO has conducted this PIA because e-Recruitment will use and maintain PII.

System: United States Coast Guard ''Biometrics at Sea''.

Component: United States Coast Guard.

Date of approval: March 14, 2008.

This PIA describes the expansion of the existing U.S. Coast Guard (USCG) and U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) Program partnership to provide mobile biometrics collection and analysis capability at sea, along with other remote areas where DHS operates. As a result of the success of this partnership's USCG Mona Pass Proof of Concept, the USCG plans a measured expansion of at-sea biometric capability throughout its mission scope and areas

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*.

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.