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 (PIA).

SUMMARY: The Privacy Office of the DHS is making available sixteen PIAs on various programs and systems in the Department. These assessments were approved and published on the Privacy Office's web site between January 8, 2011 and March 31, 2011.

DATES: The PIAs will be available on the DHS Web site until July 26, 2011, after which they may be obtained by contacting the DHS Privacy Office (contact information below).

FOR FURTHER INFORMATION CONTACT: Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, or e-mail: *pia@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: Between January 8, 2011 and March 31, 2011, the Chief Privacy Officer of the DHS approved and published sixteen 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 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: DHS/ICE/PIA–005(b) Bond Management Information System (BMIS) Web Release 2.2 Update.

Component: U.S. Immigration and Customs Enforcement (ICE).

Date of approval: January 19, 2011.

Bond Management Information System (BMIS) is an immigration bond management database used primarily by the Office of Financial Management at U.S. ICE. The basic function of BMIS is to support the financial management of immigration bonds posted for the release of aliens in ICE custody. Among other things, ICE uses BMIS to calculate and pay interest to obligors who post cash immigration bonds. Under Internal Revenue Service rules, interest payments to certain obligors are subject to backup withholdings where a percentage of the payment is withheld as tax and sent to the IRS. To begin to implement the backup withholding rules, ICE is modifying BMIS to collect additional information about obligors to determine whether a backup withholding is required. Because ICE is expanding the scope of information collected and the purposes for which BMIS information is being used, an update to the BMIS PIA is required.

System: DHS/TSA/PIA–059 TSA Advanced Imaging Technology (AIT) Update.

Component: Transportation Security Administration (TSA).

Date of approval: January 25, 2011.

TSA has deployed AIT, including backscatter x-ray and millimeter wave devices, for operational use to detect threat objects carried on persons entering airport sterile areas. AIT creates an image of the full body that highlights objects that are on the body. To mitigate the privacy risk associated with creating an image of the individual's body, TSA isolates the TSA officer (the image operator) viewing the image from the TSA officer interacting with the individual. TSA does not store any personally identifiable information from AIT screening. A PIA on the pilot was published on January 2, 2008, updated on October 17, 2008 and updated again on July 23, 2009 as program developments warranted.

TSA plans to test, and implement as appropriate, Automatic Target Recognition software for AIT machines that display anomalies on a generic figure, as opposed to displaying the image of a specific individual's body. Since the technology uses a generic image that provides greater privacy protections for the individual being screened, systems using Automatic Target Recognition will not isolate the operator viewing the image from the individual being screened. Individuals will continue to be given the option of undergoing a physical screening as an alternative to AIT screening.

System: DHS/USCIS/PIA–034 H–1B Visa Cap Registration Notice of Proposed Rule Making (NPRM).

Component: U.S. Citizenship and Immigration Services (USCIS).

Date of approval: January 28, 2011.

USCIS is proposing to amend its regulation governing petitions by U.S. employers seeking H–1B nonimmigrant worker status for aliens subject to annual numerical limitations or exempt from numerical limitations by having earned a U.S. master's or higher degree (also referred to as the ''65,000 cap'' and ''20,000 cap'' respectively, or the ''cap'' collectively). Under the proposed rule, USCIS would establish H–1B Cap Registration, a mandatory registration process, to streamline the administration of H–1B petitions filed by employers. This PIA is being conducted because the H–1B Cap Registration NPRM proposes a change to USCIS' collection of PII.

System: DHS/OPS/PIA–009 National Operations Center (NOC) Tracker and Senior Watch Officer Logs.

Component: Office of Operations Coordination and Planning (OPS).

Date of approval: February 3, 2011.

NOC in the Office of Operations Coordination and Planning (OPS) operates the NOC Tracker Log and the Senior Watch Officer (SWO) Log. The SWO Log is a synopsis of all significant information received and actions taken during a shift by the SWO. The NOC Tracker Log is a repository of all NOC responses to threats or incidents and significant activities that require a NOC tracking number. OPS has conducted this PIA because both the SWO Log and NOC Tracker Log may contain PII associated with an administrative note or a watch desk Request for Information.

System: DHS/USCIS/PIA–035 Migrant Information Tracking System.

Component: U.S. Citizenship and Immigration Services (USCIS).

Date of approval: February 3, 2011.

USCIS developed the Migrant Information Tracking System (MITS) to serve as a centralized repository for information relating to migrants interdicted at sea. MITS facilitates USCIS' ability to record and track information pertaining to a migrant's illicit maritime migration into the United States and respond to information requests regarding interdicted migrants from Members of Congress inquiring on behalf of a family member of the migrant. USCIS conducted this PIA because MITS collects, uses, and disseminates PII.

System: DHS/ALL/PIA–034 Medical Credentials Management System.

Component: Office of Health Affairs (OHA).

Date of approval: February 10, 2011.

DHS Office of Health Affairs (OHA) is instituting a centralized medical credentialing system for DHS employees that provide health care services as part of their job and the Components' mission or incidental to their ongoing operations. The purpose of the program is to formalize a process for verifying DHS employee and/or applicant qualifications, licensure information, and relevant health care provider data. In accordance with the DHS Directive 248–01, Medical Quality Management, the Assistant Secretary for Health Affairs and Chief Medical Officer (ASHA/CMO) is responsible for developing a centralized credentials management system for approving credentials for DHS employee medical care providers. The credentialing process will include the collection of and maintenance of information related to professional education, state license number(s), national registry certification, board certification, training and other pertinent information related to medical care practices. OHA conducted this PIA because the medical credentials management system will collect and maintain PII on DHS medical care providers.

System: DHS/USCG/PIA–015 Merchant Mariner Licensing and Documentation System (MMLD).

Component: United States Coast Guard.

Date of approval: March 1, 2011.

USCG owns and operates the MMLD System. The USCG uses MMLD to manage the issuance of credentials to Merchant Mariners and process merchant mariner applications; to produce merchant mariner credentials; to track the who of merchant mariner credentials issued by the USCG; to track the status of merchant mariners with respect to service, training, credentials, and qualifications, related to the operation of commercial vessels; to qualify merchant mariners for benefits and services administered by other agencies; and to perform merchant mariner call-ups related to national security. The records include the credential, background check, and medical status on each U.S. Mariner and World War II Merchant Mariner Veteran. USCG has conducted this PIA because MMLD collects and uses PII.

System: DHS/S&T/PIA–021 Cell All Demonstration.

Component: Science and Technology (S&T).

Date of approval: March 2, 2011.

The Cell All project is a research, development, testing and evaluation effort funded by the Homeland Security Advanced Research Projects Agency in the DHS S&T Directorate. Cell All is an environmental surveillance system that uses a typical cell phone as a platform for a sensor system to detect harmful chemical substances and transmit critical information, including location data, to first responder and other related monitoring agencies. With the sensors suite developed and fitted on a cell phone, S&T will conduct a demonstration of the prototype system using research-owned devices. While no PII will be collected during the demonstration, S&T is conducting a PIA to address the privacy impact of the transmission of location data using the prototype.

System: DHS/ALL/PIA–035 Nebraska Avenue Complex CCTV System.

Component: Management.

Date of approval: March 2, 2011.

The DHS, Office of the Chief Security Officer (OCSO), Physical Access Security Division (PHYSD) operates the Physical Access Control System (PACS). PACS is designed to coordinate access control, intrusion detection, and video surveillance at DHS Headquarters (HQ) facilities in the National Capital Region (NCR), primarily the Nebraska Avenue Complex (NAC). This PIA will focus exclusively on the video surveillance function within PACS known as the Closed-Circuit Television (CCTV) system at the NAC. The OCSO has conducted this PIA to analyze PII that the video surveillance function within PACS collects, uses, and maintains.

The NAC CCTV system is a video-only recording system installed at NAC. The NAC CCTV system does not have audio recording capability. The purpose of the system is to enable OCSO PHYSD and its Force Protection Branch personnel, including security guards, the ability to obtain current state visual information as well as information on or related to a security-related incident that is happening or has happened and to deter criminal activities.

System: DHS/USCIS/PIA–036 E–Verify Self Check Service.

Component: USCIS.

Date of approval: March 3, 2011.

USCIS Verification Division has developed a new service called E–Verify Self Check. The E–Verify Self Check service is voluntary and available to any individual who wants to check his own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E–Verify process. When an individual uses the E–Verify Self Check service he will be notified that either (1) his information matched the information contained in federal databases and would be deemed work-authorized, or (2) his information was not matched to information contained in federal databases which would be considered a ‘‘mismatch.’’ If the information was a mismatch, he will be given instructions on where and how to correct his records. USCIS conducted this PIA because E–Verify Self Check will collect and use PII.

System: DHS/ALL/PIA–036 DHS-wide Use of Unidirectional Social Media Applications Communications and Outreach.

Component: DHS Wide.

Date of approval: March 8, 2011.

Unidirectional social media applications encompass a range of applications, often referred to as applets or widgets that allow users to view relevant, real-time content from predetermined sources. DHS or Department intends to use unidirectional social media tools including desktop widgets, mobile apps, podcasts, audio and video streams, Short Message Service texting, and Really Simple Syndication feeds, among others, for external relations (communications and outreach) and to disseminate timely content to the public about DHS initiatives, public safety, and other official activities and one-way notifications. These dynamic communication tools broaden the Department's ability to disseminate content and provide the public multiple channels to receive and view content. The public will continue to have the option of obtaining comparable content and services through the Department's official Web sites and other official means. This PIA analyzes the Department's use of unidirectional social media applications. This PIA does not cover users sending content to the Department. Additionally, this PIA will describe the PII and the extremely limited circumstances under which the Department will have access to PII, how it will use the PII, what PII is retained and shared, and how individuals can gain access to their PII. Appendix A of this PIA will serve as a listing, to be updated periodically, of DHS unidirectional social media applications, approved by the Chief Privacy Officer, that follow the requirements and analytical understanding outlined in this PIA. The unidirectional social media applications listed in Appendix A are subject to Privacy Compliance Reviews by the DHS Privacy Office.

System: DHS/ALL/PIA–037 SharePoint.

Component: DHS Wide.

Date of approval: March 22, 2011.

DHS is developing SharePoint as a Service (SharePoint), which will be an enterprise offering available to all organizations within the Department. This platform will serve as an enterprise collaboration and communication solution, eliminating additional investments in duplicative collaborative technologies, leveraging economies of scale, and connecting separate organizations through the use of the same platform in an integrated environment. DHS is conducting this PIA because PII may be collected and stored in the SharePoint environment. This PIA sets out the minimum standard for SharePoint privacy and security requirements; DHS components may build more detailed controls and technical enhancements into their respective sites.

System: DHS/ALL/PIA038 Integrated Security Management System (ISMS).

Component: Office of Security.

Date of approval: March 23, 2011.

ISMS is a web-based case management tool designed to support the lifecycle of DHS personnel security, administrative security, and classified visit management programs. Classified visit management is an administrative process in which an individual's security clearance information is exchanged between agencies to document an individual's security clearance level. Personnel security records maintained in ISMS include suitability and security clearance investigations which contain information related to background checks, investigations, and access determinations. For administrative security and classified visit management ISMS contains records associated with security container/document tracking, classified contract administration, and incoming and outgoing classified visitor tracking. The system is a DHS enterprise-wide application that replaces the Personnel Security Activities Management System, which was decommissioned on May 31, 2010.

System: DHS/ICE/PIA–026 Federal Financial Management System (FFMS).

Component: ICE.

Date of approval: March 23, 2011.

FFMS is a web-based, workflow management and financial transaction system that provides core financial management functions for ICE and five other components within DHS: USCIS, S&T, the National Protection Programs Directorate (NPPD), Office of Health Affairs (OHA), and DHS Office of Management (MGMT). FFMS is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. The system contains personally identifiable information (PII) about DHS employees, contractors/vendors, customers and members of the public that participate in DHS programs. ICE is conducting this PIA because FFMS collects and maintains PII. This PIA focuses on ICE's collection and use of PII, and each component will publish appendices to this PIA as required to describe their collection and use of PII in FFMS.

System: DHS/ICE/PIA–027 ICE Subpoena System.

Component: ICE.

Date of approval: March 29, 2011.

The ICE Subpoena System (ISS) is owned and operated by the Office of Homeland Security Investigations (HSI) within U.S. ICE, a component of the DHS. ISS automates the process of generating, logging, and tracking subpoenas and summonses that ICE issues in furtherance of its investigations into violations of customs and immigration laws. It also supports the generation of Form I–9 notices, which notify employers that ICE intends to inspect their records to determine if they have completed the required employment eligibility forms for their employees. ICE is conducting this PIA because ISS contains PII about the individuals to whom these subpoenas, summonses, and notices are directed as well as the individuals who are the subjects of these legal process documents.

System: DHS/MGMT/PIA–005 Foreign National Visitor Management System (FNVMS).

Component: Office of Security.

Date of approval: March 30, 2011.

FNVMS, a module hosted on the DHS ISMS information technology platform, is a risk assessment tool that provides the DHS with an application to log, track, and review non-U.S. Persons (foreign nationals) who visit or perform work at DHS facilities.

Dated: May 18, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–13247 Filed 5–26–11; 8:45 am]

BILLING CODE 9110–9L–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2011–0255]

Notification of the Imposition of Conditions of Entry for Certain Vessels Arriving to the United States From the Union of the Comoros and the Republic of Cote d'Ivoire

AGENCY: Coast Guard, DHS.

ACTION: Notice.

SUMMARY: The Coast Guard announces that it will impose conditions of entry on vessels arriving from the countries of the Union of the Comoros and the Republic of Cote d'Ivoire.

DATES: The policy announced in this notice will become effective June 10, 2011.

ADDRESSES: This notice is part of docket USCG–2011–0255 and is available online by going to *http://www.regulations.gov,* inserting USCG–2011–0255 in the ''Keyword'' box, and then clicking ''Search.'' The material is also available for inspection and copying at the Docket Management Facility at the U.S. Department of Transportation, Room W12–140 on the Ground Floor of the West Building, 1200 New Jersey Avenue, SE., Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329. This policy is also available at *http://www.homeport.uscg.mil* under the Maritime Security tab; International Port Security Program (ISPS Code); Port Security Advisory link.

FOR FURTHER INFORMATION CONTACT: If you have questions on this notice, call Mr. Michael Brown, International Port Security Evaluation Division, United States Coast Guard, telephone 202—372–1081. If you have questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826 or (toll free) 1–800–647–5527.

SUPPLEMENTARY INFORMATION:

Background and Purpose

Section 70110 of title 46, United States Code, enacted as part of section 102(a) of the Maritime Transportation Security Act of 2002 (Pub. L. 107–295, Nov. 25, 2002) authorizes the Secretary of Homeland Security to impose conditions of entry on vessels requesting entry into the United States arriving from ports that are not maintaining effective anti-terrorism measures. It also requires public notice of the ineffective anti-terrorism measures. The Secretary has delegated to the Coast Guard authority to carry out the provisions of this section. See Department of Homeland Security Delegation No. 0170.1, sec. 97. Previous notices have imposed or removed conditions of entry on vessels arriving from certain countries, and those conditions of entry and the countries they pertain to remain in effect unless modified by this notice.

The Coast Guard has determined that ports in the Union of the Comoros and the Republic of Cote d'Ivoire are not maintaining effective anti-terrorism measures. To make these determinations, the Coast Guard International Port Security (IPS) Program conducted an initial visit to the Union of the Comoros in November 2009, and conducted an initial visit to the Republic of Cote d'Ivoire in January 2010. In our investigations of both countries, significant deficiencies were found in the legal regime, designated authority oversight, access control, and cargo control. In September 2010, the Deputy Commandant for Operations made findings that effective anti-terrorism measures were not in place in the ports of Comoros and Cote d'Ivoire. Inclusive to these determinations is an assessment that the Union of the