Total Burden Hours: 850 annual burden hours.

Total Burden Cost (capital/startup): $0 .

Total Burden Cost (operating/maintaining): $20,757.

Post-Meeting/Workshop/Training Evaluation

Frequency: On occasion.

Affected Public: State, local, or Tribal government.

Number of Respondents: 5,000.

Estimated Time Per Respondent: 15 minutes.

Total Burden Hours: 1,250 annual burden hours.

Total Burden Cost (capital/startup): $0 .

Total Burden Cost (operating/maintaining): $30,525.

Dated: June 17, 2011.

David Epperson,

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

[FR Doc. 2011–16064 Filed 6–27–11; 8:45 am]

BILLING CODE 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 (PIA).

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

DATES: The PIAs will be available on the DHS Web site until August 29, 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 March 31, 2011 and May 31, 2011, the Chief Privacy Officer of the DHS approved and published ten 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 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/USCG/PIA–016 College Board Requirement Plus (CBRP).

Component: United States Coast Guard (USCG).

Date of approval: April 1, 2011.

DHS United States Coast Guard Academy (USCGA or Academy) uses College Board's *Recruitment PLUS*™ (Recruitment PLUS) software application for college admissions and enrollment activities. The Recruitment PLUS system does the following things:

1. Collects and stores prospective applicants' biographic and educational data,

2. Collects USCGA admissions staff's and volunteers' biographical data,

3. Facilitates and tracks the application process, and

4. Aligns admissions staff and volunteers to prospective applicants.

The purpose of this PIA is to document how Recruitment Plus collects and uses personally identifiable information (PII).

System: DHS/NPPD/PIA–012 Critical Infrastructure Warning Information Network (CWIN).

Component: National Protection & Programs Directorate (NPPD).

Date of approval: April 11, 2011.

The CWIN system has undergone a PIA 3-Year Review requiring no changes and continues to accurately relate to its stated mission. DHS NPPD examined the privacy implications for CWIN. DHS is responsible for protecting the national infrastructures and responsible for ensuring that in the event cyber or physical infrastructures are compromised, there is a means to collaborate and coordinate the necessary resources to restore impacted infrastructures. The mission of CWIN is to facilitate immediate alert, notification, sharing and collaboration of critical infrastructure and cyber information within and between Government and industry partners. CWIN provides a technologically advanced, secure network for communication and collaboration, and alert and notification. CWIN is DHS' only survivable, critical communications tool not dependent on the Public Switch Network or the public Internet that can communicate both data and voice information in a collaborative environment in support of infrastructure restoration. CWIN provides a survivable, dependable method of communication allowing DHS to communicate with other Federal agencies, state and local government, the private sector, and international organizations in the event that primary methods of communication are unavailable.

CWIN members belong to one of the vital sectors of the national infrastructure as named in the National Response Plan, appears in the Interim National Infrastructure Protection Plan, or are a state Homeland Security Advisor. Only CWIN members have access to CWIN. CWIN membership is by invitation only, with invitations issued from the Infrastructure Coordination Division Director through a contractor. The CWIN operation consists of the collection of point of contact information for administrative purposes, and the placement of a CWIN terminal at member locations. Should an event occur where traditional communication methods are not operable, CWIN provides a communication method between key infrastructure sites across the country.

System: DHS/NPPD/PIA–009 Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program.

Component: NPPD.

Date of approval: May 4, 2011.

The DHS/NPPD/Office of Infrastructure Protection (IP)/Infrastructure Security Compliance Division (ISCD) is conducting this PIA to detail the privacy impact associated with the CFATS Personnel Surety Program and the required security assessments performed by high-risk chemical facilities in fulfillment of Risk-Based Performance Standard # 12 (6 CFR 27.230(a)(12)). This PIA describes the procedures for submitting PII on individuals impacted by this program to NPPD, and also describes NPPD's uses of that PII.

System: DHS/S&T/PIA–022 Biodefense Knowledge Management System v. 2.0 (BKMS).

Component: Science & Technology (S&T).

Date of approval: May 4, 2011.

DHS S&T Biodefense Knowledge Center (BKC) developed and operates the BKMS. The current generation of the BKMS, version 1.0, enables approved users to access and analyze biological sciences topics and related biodefense information to assist with their efforts to better understand or characterize biological threats, by offering an integrated suite of tools for managing and indexing scientific documents and information. In BKMS 2.0, S&T intends to add a component to the system to include data derived from the intelligence community (IC) and law enforcement (LE)-sensitive data. S&T is conducting this PIA because such an

addition will allow for a new function of the system for selected BKMS users, who are authorized to explore IC/LE data (which may contain PII).

System: DHS/TSA/PIA–033 Enterprise Search Portal (ESP).

Component: Transportation Security Administration (TSA).

Date of approval: May 5, 2011.

DHS TSA is implementing a search capability to enable authorized users to search or discover data held by separate databases within TSA. The search function will be known as the ESP. TSA is conducting this PIA to assess privacy impacts associated with this capability to search across multiple databases. The systems being searched are covered by other PIAs or are otherwise compliant with the E–Government Act of 2002.

System: DHS/USCIS/PIA–030(b) E–Verify RIDE Update.

Component: United States Citizenship and Immigration Services (USCIS).

Date of approval: May 6, 2011.

USCIS Verification Division has developed a new enhancement to the E–Verify Program entitled Records and Information from Department of Motor Vehicles for E–Verify (RIDE). RIDE enhances the integrity of the E–Verify Program by verifying information from the most commonly presented identity documents (*e.g.* employee's driver's license, driver's permit, or state-issued identification card) for employment authorization, when the issuing state or jurisdiction of those documents has established a Memorandum of Agreement with the DHS to participate in RIDE. USCIS is conducting this PIA update to assess the privacy risks and mitigation strategies for this new enhancement.

System: DHS/TSA/PIA–034 Enterprise Performance Management Platform (EPMP).

Component: TSA.

Date of approval: May 10, 2011.

TSA EPMP is designed to assist in performing security management functions using a wide variety of data associated with security, equipment, and screening processes from TSA's security activities. EPMP will now maintain PII about members of the public in excess of basic contact information, which requires TSA to conduct a new PIA. This PIA focuses on the portions of EPMP using PII.

System: DHS/USCG/PIA–004 Law Enforcement Information Data Base (LEIDB)/Pathfinder.

Component: USCG.

Date of approval: May 11, 2011.

The LEIDB/Pathfinder system has undergone a PIA 3-Year Review requiring no changes and continues to accurately relate to its stated mission. USCG, a component of DHS established the LEIDB/Pathfinder. LEIDB/Pathfinder archives text messages prepared by individuals engaged in USCG law enforcement, counter terrorism, maritime security, maritime safety and other USCG missions enabling intelligence analysis of field reporting. USCG has conducted this PIA because the LEIDB/Pathfinder system collects and uses PII.

System: DHS/TSA/PIA–001 Vetting and Credentialing Screening Gateway System (CSG) .

Component: TSA.

Date of approval: May 18, 2011.

The CSG system has undergone a PIA 3-Year Review and requires an update to accurately relate to its stated mission. The Consolidated Screening Gateway is the system of hardware, software and communications infrastructure used by the Transportation Security Administration to conduct security threat assessments on various transportation workers and other populations related to transportation.

System: DHS/ICE/PIA–015(b) Enforcement Integrated Database (EID) ENFORCE Alien Removal Module (EARM 3.0) Update.

Component: Immigration and Customs Enforcement (ICE).

Date of approval: May 20, 2011.

The EID is a DHS shared common database repository for several DHS law enforcement and homeland security applications. EID, which is owned and operated by U.S. ICE, captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, U.S. Customs and Border Protection (CBP), and USCIS, agencies within DHS. DHS personnel access the data in EID using the ENFORCE suite of software applications: ENFORCE Apprehension Booking Module (EABM), ENFORCE Alien Detention Module (EADM), and ENFORCE Alien Removal Module (EARM). The PIA for EID was published in January 2010 and last updated in September 2010. ICE is now deploying an upgrade to the ENFORCE applications, referred to as EARM version 3.0 (EARM 3.0), to merge two of the ENFORCE applications, and to modify the data collected by DHS, the capabilities of the software, and certain system interfaces. These changes require an update to the EID PIA.

Dated: June 20,2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–16160 Filed 6–27–11; 8:45 am]

BILLING CODE 9110–9L–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[Docket ID FEMA–2011–0009]

Agency Information Collection Activities: Submission for OMB Review; Comment Request, OMB No. 1660–0039; FEMA Form 078–0–2A, National Fire Academy (NFA) Long-Term Evaluation Student/Trainee; FEMA Form 078–0–2, NFA Long-Term Evaluation Supervisors

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice; 30-day notice and request for comments; extension, without change, of a currently approved information collection; OMB No. 1660–0039; FEMA Form 078–0–2A (Presently FEMA Form 95–59), NFA Long-Term Evaluation Student/Trainee; FEMA Form 078–0–2 (Presently FEMA Form 95–58), NFA Long-Term Evaluation Supervisors.

SUMMARY: The Federal Emergency Management Agency (FEMA) will submit the information collection abstracted below to the Office of Management and Budget for review and clearance in accordance with the requirements of the Paperwork Reduction Act of 1995. The submission will describe the nature of the information collection, the categories of respondents, the estimated burden (*i.e.,* the time, effort and resources used by respondents to respond) and cost, and the actual data collection instruments FEMA will use.

DATES: Comments must be submitted on or before July 28, 2011.

ADDRESSES: Submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, Office of Management and Budget. Comments should be addressed to the Desk Officer for the Department of Homeland Security, Federal Emergency Management Agency, and sent via electronic mail to *oira.submission@omb.eop.gov* or faxed to (202) 395–5806.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or