9110-9L

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 Department of Homeland Security (DHS) Privacy Office is making available thirty-eight Privacy Impact Assessments (PIA) on various programs and systems in the Department. These assessments were approved and published on the Privacy Office's web site between June 1, 2012, and November 30, 2012.

DATES: The PIA will be available on the DHS website until [INSERT DATE 60 DAYS AFTER PUBLICATION], after which they may be obtained by contacting the DHS Privacy Office (contact information below).

FOR FURTHER INFORMATION CONTACT: Jonathan R. Cantor, Acting Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, or email: pia@dhs.gov.

SUPPLEMENTARY INFORMATION: Between June 1, 2012, and November 30, 2012, the DHS Chief Privacy Officer and Acting Chief Privacy Officer approved and published thirty-eight PIAs on the DHS Privacy Office website, www.dhs.gov/privacy, under the link for "Privacy Impact Assessments." 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 website or by contacting the Privacy Office.

System: **DHS/S&T/PIA-025 Gaming System Monitoring and Analysis Effort**

Component: **Science and Technology Directorate (S&T)**

Date of approval: **June 1, 2012**

The Gaming System Monitoring and Analysis project is a research effort funded by the Department's S&T Cyber Security Division to design and develop forensic tools for extracting data from gaming systems. S&T conducted a PIA because gaming systems used in this research project may contain personally identifiable information (PII).

System: **DHS/CBP/PIA-006(b) Automated Targeting System (ATS)**

Component: **U.S. Customs and Border Protection (CBP)**

Date of approval: **June 1, 2012**

As a decision support tool, ATS compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. This PIA was conducted to notify the public about the changes in modules and expansion of access to datasets used by and stored in ATS.

This PIA was published in conjunction with an updated System of Records Notice, 77 FR 30297 (May 22, 2012).

System: **DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI)**

Component: **CBP**

Date of approval: **June 1, 2012**

AFI enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border. AFI is used for the purposes of: (1) identifying individuals, associations, or relationships that may pose a

potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods, or identifying other violations of law; (2) conducting additional research on persons and/or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products developed in connection with the above purposes with DHS employees who have a need to know in the performance of their official duties and who have appropriate clearances or permissions. Finished intelligence products are tactical, operational, and strategic law enforcement intelligence products that have been reviewed and approved for sharing with finished intelligence product users and authorities outside of DHS, pursuant to routine uses in the published Privacy Act System of Records Notice.

In order to mitigate privacy and security risks associated with the deployment of AFI, CBP has built technical safeguards into AFI and developed a governance process that includes the operational components of CBP, the oversight functions of the CBP Privacy Officer and Office of Chief Counsel, and the Office of Information and Technology. Additionally, the DHS Privacy Office provides oversight for the program.

This PIA was necessary because AFI accesses and stores PII retrieved from DHS, other federal agency, and commercially available databases.

System: **DHS/FEMA/PIA-027 Accounting Package (ACCPAC)**

Component: **Federal Emergency Management Agency (FEMA)**

Date of approval: **June 8, 2012**

FEMA, Office of the Chief Financial Officer, Debt Establishment Unit, owns and operates the ACCPAC application. ACCPAC is a commercial-off-the-shelf product that assists FEMA Accounts Receivable personnel in tracking, monitoring, and managing debts owed to the Agency. FEMA conducted this PIA because ACCPAC collects, uses, maintains, retrieves, and disseminates PII, including Employer Identification Numbers and Social Security Numbers, to perform its tasks.

System: **DHS/FEMA/PIA-027 National Emergency Management Information System-Individual Assistance (NEMIS-IA) Web-based and Client-based Modules**

Component: **FEMA**

Date of approval: **June 29, 2012**

FEMA, Office of Response and Recovery, Recovery Directorate, and National Processing Service Center Division operate the National Emergency Management Information System (NEMIS) Individual Assistance (IA) system. NEMIS-IA supports FEMA's recovery mission under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. 93-288, as amended, by processing information obtained from disaster recovery assistance applications via the Disaster Assistance Improvement Program/Disaster Assistance Call Center system. NEMIS-IA, which consists of both client-based and web-based modules, also utilizes business rules to detect and prevent "duplication of benefits." FEMA conducted this PIA because NEMIS-IA collects, uses, maintains, retrieves, and disseminates the PII of applicants to FEMA's disaster recovery individual assistance programs.

System: **DHS/FEMA/PIA-026 Operational Data Store (ODS) and Enterprise Data Warehouse (EDW) systems**

Component: **FEMA**

Date of approval: **June 29, 2012**

FEMA and the Office of the Chief Information Officer own and operate the ODS and EDW systems. ODS and EDW replicate source system-provided data from other operational FEMA systems and provide a simplified way of producing Agency reports for internal use as well for external stakeholders. These reports relate to FEMA mission activities, such as FEMA's readiness to deploy, disaster response, internal operations, and oversight. Reports are based on the needs of the particular program requirements or mission-related activity. Each source system has a separate data mart within the ODS to ensure that information is not commingled and that the source system rules for use are followed within the ODS. Data marts allow for the manipulation of data while at the same time ensuring that the exact same data within the source system remains static. FEMA conducted this PIA because ODS and EDW collect, use, maintain, retrieve, and disseminate PII pulled from the source systems.

System: **DHS/FEMA/PIA-025 Hazard Mitigation Grant Program (HMGP) System**

Component: **FEMA**

Date of approval: **June 29, 2012**

FEMA's Federal Insurance and Mitigation Administration (FIMA) operates the HMGP system. The HMGP system is a grant application and management system. FEMA conducted this PIA because the FEMA FIMA HMGP system may collect, use, maintain,

retrieve, and disseminate the PII of grantees or sub-grantees as well as the PII of individual property owners associated with the grants or sub-grants.

System: **DHS/ALL/PIA-042 Department of Homeland Security (DHS) Closed-Circuit Television (CCTV)**

Component: **DHS-wide**

Date of approval: **July 18, 2012**

DHS and its components deploy a number of CCTV systems throughout the Department. DHS' CCTV systems are used to obtain real-time and recorded visual information in and around federal worksites and facilities to aid in crime prevention and criminal prosecution, enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation and terrorism prevention. DHS conducted this PIA because these systems have the ability to capture images of people, license plates, and other visual information within range of the cameras. This PIA replaced existing CCTV PIAs. Those PIAs were retired with the publication of this PIA and are listed in an appendix.

System: **DHS/ICE/PIA-010(a) The National Child Victim Identification System (NCVIS)**

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

Date of approval: **July 18, 2012**

NCVIS is owned by ICE, Homeland Security Investigations (HSI), and is an application that assists federal, state, local, and international law enforcement agencies, INTERPOL, and other supporting organizations, such as the National Center for Missing and Exploited Children (hereafter, authorized partners) in the investigation and prosecution of

child exploitation crimes, specifically those involving images of child sexual exploitation. NCVIS maintains a repository of digital images of child exploitation seized and/or submitted to ICE for comparison by law enforcement agencies. These images may capture the faces or other identifying features of the victims and violators involved in these crimes. HSI is expanding the scope of system information that is shared with authorized partners that maintain their own databases of images related to child exploitation crimes for the purposes of identifying the child victims and supporting law enforcement investigations and prosecutions of these crimes. This expanded sharing is intended to allow law enforcement personnel to use these images during investigations to identify and rescue child victims as well as to identify and prosecute the perpetrators of these crimes. HSI is also expanding the range of images shared with law enforcement agencies that have requested a matching report of an image submitted for NCVIS comparison. The PIA for NCVIS was originally published on August 21, 2009. Because HSI is expanding the scope of NCVIS information that is shared with authorized partners, an update to the NCVIS PIA was required.

System: **DHS/NPPD/PIA-021(a) Joint Cybersecurity Services Program Defense Industrial Base (DIB) – Enhanced Cybersecurity Services (DECS)**

Component: **National Protection and Programs Directorate (NPPD)**

Date of approval: **July 18, 2012**

The Joint Cybersecurity Services Pilot (JCSP) is the Department's voluntary information sharing initiative with the Department of Defense (DOD) and participating commercial companies. NPPD is updating the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA published on January 13, 2012, to reflect

the establishment of the JCSP as an ongoing permanent program (now known as the Joint Cybersecurity Services Program (JCSP)). The purpose of the program is to enhance the cybersecurity of participating critical infrastructure entities through information sharing partnerships with the critical infrastructure organization or their Commercial Service Provider (CSP). The first phase of the JCSP will focus on the cyber protection of the Defense Industrial Base (DIB) companies that are participating in the DoD's Cyber Security/Information Assurance (CS/IA) Program. This sub-program is known as the DIB Enhanced Cybersecurity Services (DECS). The JCSP may also be used to provide equivalent protection to participating Federal civilian agencies pending deployment of EINSTEIN intrusion prevention capabilities.

System: **DHS/CBP/PIA-007(b) Electronic System for Travel Authorization (ESTA)**

Component: **CBP**

Date of approval: **July 18, 2012**

CBP published this update to the PIA for ESTA, last updated July 18, 2011. ESTA is a web-based application and screening system used to determine whether certain aliens are eligible to travel to the United States under the Visa Waiver Program. CBP conducted this updated PIA to evaluate the privacy impact of including the Internet Protocol address associated with a submitted ESTA application for vetting purposes, as well as to evaluate the privacy impact of various updates to the ESTA System of Records Notice, including updates and clarifications to the routine uses and a new routine use permitting the sharing of information in connection with judicial proceedings.

System: **DHS/TSA/PIA-037 Automated Wait Time (AWT)**

Component: **Transportation Security Administration (TSA)**

Date of approval: **July 22, 2012**

TSA will test and deploy systems automating the collection of information to calculate passenger average wait time in the checkpoint queue. TSA's AWT system utilizes information broadcast from Bluetooth®-enabled devices carried by individuals in the general checkpoint queuing area to calculate wait times and deploy resources, as appropriate, to reduce delays in checkpoint queues. In the interest of transparency to the public, this PIA was conducted pursuant to Section 222 of the Homeland Security Act to assess privacy risk from the AWT system. In order to ensure that AWT systems sustain and do not erode privacy protections, TSA developed and implemented processes that give effect to the Fair Information Practice Principles while generating statistical data used for improving checkpoint operations.

System: **DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT**

Component: **CBP**

Date of approval: **July 25, 2012**

CBP has established E3, the CBP portal to U.S. Immigration and Customs Enforcement's Immigration and Enforcement Operational Records System, Enforcement Integrated Database and US-VISIT's Automated Biometric Identification System (IDENT), to collect and transmit data related to law enforcement activities. E3 collects and transmits biographic, encounter, and biometric data including, but not limited to, fingerprints for identification and verification of individuals encountered at the border for CBP's law enforcement and immigration mission. In addition to the collection of fingerprints, beginning at the end of July 2012, the E3 portal began a six-week pilot program to collect iris scans of individuals apprehended by CBP Border Patrol at the McAllen, Texas,

Border Patrol Station. Collection of iris scans provides the capability to capture biometric data from individuals if their fingerprints cannot be obtained, and also to biometrically compare and authenticate an individual's identity. In different operational environments, iris scans can be captured more quickly than fingerprints, are as or more reliable in providing a unique biometric, do not involve the touching of the subject with respect to those cultures for whom such contact poses a concern, and require less storage capacity and transmission bandwidth than fingerprints. This PIA was conducted because E3 requires the collection of PII.

System: **DHS/ICE/PIA-015(e) Enforcement Integrated Database (EID) – EAGLE**

Component: **ICE**

Date of approval: **July 25, 2012**

ICE has established a new subsystem within EID called EID Arrest Guide for Law Enforcement (EAGLE). EAGLE is a booking application used by ICE law enforcement officers to process the biometric and biographic information of individuals arrested by ICE for criminal violations of law and administrative violations of the Immigration and Nationality Act. Once fully deployed, EAGLE will replace the existing EID booking applications, the Enforcement Apprehension and Booking Module, Mobile IDENT, and WebIDENT, and will perform the identical functions of those applications as described below and in the EID PIA. EAGLE will also forge a new connection to the Department of Defense's (DOD) Automated Biographic Information System (ABIS) and permit the comparison of the fingerprints of foreign nationals arrested by ICE with the DOD's information in ABIS. This PIA update was conducted to provide public notice of the

operation of the EAGLE booking system and its interconnection to the DOD ABIS database.

System: **DHS/OPS/PIA-008 Homeland Security Information Network R3 User Accounts (HSIN)**

Component: **Operations Coordination and Planning (OPS)**

Date of approval: **July 25, 2012**

HSIN is maintained by the Department of Homeland Security, OPS. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources among federal, state, local, tribal, private-sector commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism as well as in undertaking incident management activities. HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. OPS conducted this PIA because HSIN collects PII in the form of user account registration information from HSIN users in order to allow them access to the HSIN Release 3 (R3) community.

System: **DHS/OPS/PIA-007 Homeland Security Information Network 3.0 Shared Spaces**

Component: **OPS**

Date of approval: **July 25, 2012**

OPS maintains HSIN on the Sensitive but Unclassified network. HSIN is designed to facilitate the secure integration and interoperability of information-sharing resources between federal, state, local, tribal, territorial, private sector, international, and other non-governmental partners involved in identifying and preventing terrorism as well as in

undertaking incident management activities. HSIN is a user-driven, web-based, information-sharing platform that connects all homeland security mission partners within a wide spectrum of homeland security mission areas. OPS conducted this PIA because the substantive material posted and shared within the HSIN collaboration spaces contains PII about members of the public who are the subject of documents, reports, or bulletins contained in those spaces.

System: **DHS/NPPD/PIA-009 Chemical Facility Anti-Terrorism Standards (CFATS)**

Component: **NPPD**

Date of approval: **July 26, 2012**

NPPD consolidated and updated this PIA for the CFATS regulations, 6 CFR Part 27. This PIA replaced the former PIAs for the Chemical Security Assessment Tool and CFATS, in order to provide a unified analysis of the collection and use of PII as part of CFATS. CFATS is the DHS regulation that governs security at high-risk chemical facilities and represents a national-level effort to minimize terrorism risk to such facilities.

System: **DHS/USCIS/PIA-006(a) Systematic Alien Verification for Entitlements (SAVE)**

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

Date of approval: **July 27, 2012**

USCIS's Verification Division published an update to the SAVE Program PIA dated August 26, 2011. SAVE is a fee-based, inter-governmental initiative designed to help

federal, state, tribal, and local government agencies confirm immigration status prior to the granting of benefits and licenses, as well as for other lawful purposes. USCIS updated this PIA to: (1) describe the new collection of foreign passport country of issuance from agencies issuing benefits and from the United States Visitor and Immigrant Status Indicator Technology Arrival and Departure Information System, (2) describe the addition of Enterprise Citizenship and Immigration Services Centralized Operational Repository, (3) describe the decommissioning of the Image Storage and Retrieval System and replacement by the Customer Profile Management System, and (4) describe the decommissioning of the Reengineered Naturalization Applications Casework System and replacement by Claims Linked Application Information Management System 4.

System: **DHS/USCIS/PIA-030(d) E-Verify Program**

Component: **USCIS**

Date of approval: **July 27, 2012**

USCIS's Verification Division published an update to the DHS/USCIS-030 E-Verify Program PIA. USCIS administers the E-Verify program, which allows participating employers the ability to verify the employment eligibility of all newly hired employees. USCIS updated this PIA to: (1) describe collection and verification of the foreign passport country of issuance through the U.S. Visitor and Immigrant Status Indicator Technology program's Arrival and Departure Information System, and (2) discuss the decommissioning of the Image Storage and Retrieval System (ISRS) and the Reengineered Naturalization Applications Casework System (RNACS) subsystems. The functionality previously provided by ISRS and RNACS will be replaced by the Customer

Profile Management System and Claims Linked Application Information Management System 4, respectively.

System: **DHS/USCIS/PIA-036(a) Employment Eligibility Verification Requirements Under the Form I-9**

Component: **USCIS**

Date of approval: **July 27, 2012**

The Verification Division of USCIS manages the business process in support of the statutory requirement that employers in the United States complete and maintain the Form I-9, *Employment Eligibility Verification*, to identify and verify employment authorization for all of their new employees. While the recent rulemakings that implemented changes to the Form I-9 did not impact what information DHS collects directly from individuals, which would trigger the requirement for a PIA, under the E-Government Act, USCIS conducted this PIA to provide more transparency into the design and use of the Form I-9, a key aspect of the employment eligibility verification process.

System: **DHS/TSA/PIA-030(a) Access to Sensitive Security Information (SSI) in Contract Solicitations**

Component: **TSA**

Date of approval: **July 27, 2012**

TSA currently conducts security threat assessments (STA) on individuals and companies that seek access to SSI necessary to prepare a proposal in the pre-contract award phase of contracting with TSA. SSI is a form of unclassified information that if publicly released would be detrimental to transportation security. The standards governing SSI are

promulgated under 49 U.S.C. §114(r) in 49 CFR. part 1520. There may, however, also be circumstances under which individuals and companies will require access to SSI in order to prepare a proposal for contracts with other governmental agencies (federal, state, or local level) or with private industry. TSA updated this PIA to reflect that TSA will perform STA on individuals and companies seeking access to SSI in order to prepare a proposal with such other entities.

System: **DHS/OPS/PIA-009 National Operations Center Operations Counterterrorism Desk (NCOD) Database**

Component: **OPS**

Date of approval: **July 30, 2012**

The National Operations Center (NOC), within OPS, operates the NOC Counterterrorism Operations Desk (NCOD) and serves as the primary Department of Homeland Security point of contact to streamline counterterrorism Requests for Information (RFI). The NCOD Database is a tracking tool used by NCOD Officers to track all counterterrorism related incoming and outgoing inquiries. OPS conducted this PIA because the NCOD Database contains PII.

System: **DHS/NPPD/PIA-026 National Cybersecurity Protection System (NCPS)**

Component: **NPPD**

Date of approval: **July 30, 2012**

NCPS is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend the federal civilian government agencies' information technology infrastructure from cyber threats. The NCPS includes the hardware, software, supporting processes, training, and services that are developed

and acquired to support its mission. NPPD conducted this PIA because PII may be collected by the NCPS, or through submissions of known or suspected cyber threats received by US-CERT for analysis. This PIA will serve as a replacement for previously published PIAs submitted by NSCD for the 24/7 Incident Handling Center (March 29, 2007), and the Malware Lab Network (May 4, 2010), and is a program-focused PIA to better characterize the efforts of NCPS and US-CERT.

System: **DHS/USCIS/PIA-044 Fraud Detection and National Security Directorate (FDNS)**

Component: **USCIS**

Date of approval: **July 30, 2012**

USCIS created the FDNS to strengthen the integrity of the nation's immigration system and to ensure that immigration benefits are not granted to individuals that may pose a threat to national security and/or public safety. In addition, the FDNS is responsible for detecting, deterring, and combating immigration benefit fraud. USCIS conducted this PIA to document and assess how the FDNS collects, uses, and maintains PII.

System: **DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals**

Component: **USCIS**

Date of approval: **August 14, 2012**

On June 15, 2012, Secretary of Homeland Security Janet Napolitano (the Secretary) issued a DHS memorandum entitled, "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children." The Secretary addressed the memorandum to the Acting Commissioner of U.S. Customs and Border Protection, and

to the Directors of USCIS and U.S. Immigration and Customs Enforcement. The Secretary's memorandum set forth how prosecutorial discretion may be exercised in cases involving certain people who arrived in the United States as children. The Secretary emphasized that generally, this population lacked the intent to violate the law, and that her memorandum would ensure enforcement resources would not be expended on these low priority cases.

The basis for the Secretary's memorandum is the Secretary's authority to exercise prosecutorial discretion by deferring action in appropriate cases. Prosecutorial discretion is the authority to determine how and when to exercise enforcement authority in line with agency priorities. Deferred action is an exercise of this prosecutorial discretion to defer removal action against certain individuals who are unlawfully present in the United States in order to devote scarce enforcement resources to the highest priority removal cases, including individuals who pose a danger to national security or public safety or have been convicted of specific crimes. USCIS published this PIA because the deferred action for childhood arrivals process associated with this memorandum involves the collection and use of PII.

System: **DHS/ALL/PIA-042 Department of Homeland Security (DHS) Personal Identity Verification (PIV)**

Component: **DHS-Wide**

Date of approval: **August 23, 2012**

DHS updated the PIV Privacy Impact Assessment Update to reflect changes in Departmental requirements and enhanced interoperability with US-VISIT Automated

Biometric Identification System and the Federal Bureau of Investigation Criminal Justice Information Services, Integrated Automated Fingerprint Identification System, DHS Component Physical Access Control Systems, DHS Component Active Directories, as well as issuance of PIV-compatible credentials to visitors to DHS.

System: **DHS/S&T/PIA-001(a) Border Network (BorderNet) and Northeast Test Bed (NET-B)**

Component: **S&T**

Date of approval: **August 23, 2012**

BorderNet (formerly named the Border and Transportation Security Network, or BTSNet) is a technology test bed developed and maintained by the Department of Homeland Security (DHS), Science and Technology Directorate (S&T) located at the United States-Mexico border. The purpose of the test bed is to test and evaluate technologies in an operational environment that assist DHS Customs and Border Protection field agents in securing our nation's borders. S&T updated this PIA to reflect the addition of mobile enrollment technology and surveillance cameras, and the deployment of an additional test bed site at the United States-Canada border, called NET-B.

System: **DHS/S&T/PIA-024 Rapid Deoxyribonucleic Acid (DNA) System**

Component: **S&T**

Date of approval: **September 14, 2012**

S&T developed the Rapid DNA System primarily to meet the need of U.S. Citizenship and Immigration Services (USCIS) to verify family relationships in refugee immigration

processes. The Rapid DNA System performs rapid, low-cost DNA analysis to meet this USCIS need and may also address operational needs of other DHS components. S&T conducted this PIA because the collection and analysis of DNA information raises potential privacy concerns.

System: **DHS/TSA/PIA-038 Performance and Results Information System (PARIS)**

Component: **TSA**

Date of approval: **September 18, 2012**

TSA PARIS system is a database used for maintaining information associated with TSA's regulatory investigations, security incidents, and enforcement actions, as well as for recording the details of security incidents involving passenger and property screening. PARIS maintains PII about individuals, including witnesses, involved in security incidents or regulatory enforcement activities. PARIS also creates and maintains a list of individuals who, based upon their involvement in security incidents of sufficient severity or frequency, are disqualified from receiving expedited screening for some period of time or permanently. The purpose of this PIA is to inform the public of changes in the use of PARIS and any resulting impact to personal privacy.

System: **DHS/CBP/PIA-004(f) Western Hemisphere Travel Initiative (WHTI)**

Component: **CBP**

Date of approval: **September 24, 2012**

CBP published this PIA to give notice of an update to the WHTI PIA. This update describes Phase I of the Beyond the Border entry/exit program, which is an initiative of the U.S.-Canada Beyond the Border Action Plan. The Beyond the Border entry/exit

program will expand the sharing of border crossing information with the Canada Border Services Agency by exchanging biographic, travel document, and other border crossing information collected from individuals entering the United States from Canada and vice versa at land ports of entry. This exchange of border crossing entry information will assist both countries so that the record of an entry into one country establishes an exit record from the other, ultimately supporting each nation in their immigration and law enforcement missions, as well as facilitating cross-border travel. This PIA update covered Phase I of the entry/exit program only, which is limited to exchanging entry records from certain individuals (other than U.S. and Canadian citizens) at certain land ports of entry to measure the ability to reconcile biographic entry records between Canada and the United States. DHS will publish additional updates to this PIA in advance of deployment of any subsequent phases to the Beyond the Border entry/exit program.

System: **DHS/NPPD/PIA-011 Federal Protective Service (FPS) Information Support Tracking System (FISTS)**

Component: **National Protection and Programs Directorate (NPPD)**

Date of review: **October 4, 2012**

This PIA was reviewed using the three-year PIA checklist. U.S. Immigration and Customs Enforcement (ICE), Federal Protective Service (FPS), Information Support Tracking System (FISTS), Contract Suitability Module is a web-based application used to automate the process for assessing the suitability of FPS and General Services Administration contract personnel to work in secure Federal buildings, and to track periodic background re-investigations of those contract employees. The system collects and maintains information on applicants and contractor personnel who work in secure

Federal buildings such as security officers, childcare workers, cleaners, and other contracted service positions. FPS conducted this PIA because FISTS collects and uses PII on members of the public who seek or are currently employed in these positions within Federal facilities.

System: **DHS/FEMA/PIA-011 National Flood Insurance Program Information Technology System**

Component: **FEMA**

Date of approval: **October 12, 2012**

DHS FEMA FIMA National Flood Insurance Program (NFIP) owns and operates the NFIP Information Technology System (ITS). The NFIP ITS processes flood insurance policies and claims, specifically, policies and claims from the FEMA Direct Servicing Agent (DSA) contractor on behalf of the NFIP and by Write Your Own Companies (WYO) that sell and service flood insurance policies. An NFIP flood insurance policy can be obtained directly from a DSA through a licensed insurance broker or from WYOs. Since 1983, participating insurance companies have delivered and serviced NFIP policies in their own names, through the "Write Your Own" arrangement. The policy coverage and premiums do not differ if purchased from the DSA or WYOs. FEMA conducted this PIA because NFIP ITS collects, uses, maintains, retrieves, and disseminates PII about individuals who purchase, as well as those who process, flood insurance policies from NFIP and individuals requesting access to the system.

System: **DHS/TSA/PIA-040 Port Authority of New York/New Jersey (PANYNJ) Secure Worker Access Consortium Vetting Services (SWAC)**

Component: **TSA**

Date of approval: **November 13, 2012**

TSA will conduct terrorism watch list checks of workers at PANYNJ facilities and job sites, including critical infrastructure such as airports, marine ports, bus terminals, rail transit facilities, bridges, tunnels, and real estate such as the World Trade Center memorial site. TSA will also conduct terrorism watch list checks of individuals identified by PANYNJ as requiring such checks for access to sensitive information, and for workers at facilities and job sites of PANYNJ regional partners. Results of the checks will not be reported to PANYNJ, but instead will be forwarded to the Federal Bureau of Investigation Terrorist Screening Center. This PIA was conducted pursuant to the E-Government Act of 2002 because PII will be collected to conduct terrorism watch list checks of workers at PANYNJ facilities and job sites.

System: **DHS/TSA/PIA-039 Trends and Patterns Branch (TPB)**

Component: **TSA**

Date of approval: **November 13, 2012**

TSA, Trends and Patterns Branch (TPB) seeks to improve the ability to identify potential risks to transportation security by discovering and analyzing previously unknown links or patterns among individuals who undergo a TSA security threat assessment, aviation passengers identified as a match to a watch list, and passengers who do not present acceptable identification documents to access the sterile area of an airport whose identity is unverified. TSA conducted this PIA because the TPB will collect and use PII to perform these functions.

System: **DHS/FEMA/PIA-012(a) Disaster Assistance Improvement Program (DAIP)**

Component: **FEMA**

Date of approval: **November 16, 2012**

FEMA, Office of Response & Recovery, Recovery Directorate, National Processing Service Center Operations Branch, sponsors and funds the DAIP. In accordance with Executive Order 13411 "Improving Assistance for Disaster Victims," DAIP developed the Disaster Assistance Center (DAC) system. As a part of DAIP, DAC maintains disaster survivor application and registration information collected through various media including: (1) DAIP paper forms, (2) the www.disasterassistance.gov website, (3) the http://m.fema.gov mobile website, and (4) via telephone. DAIP/DAC shares the information with the National Emergency Management Information System– Individual Assistance (IA) module to facilitate eligibility determinations and with other federal, tribal, state, local, and non-profit agencies/organizations that also service disaster survivors. FEMA conducted this PIA because DAIP/DAC collects, uses, maintains, retrieves, and disseminates PII of disaster survivors who either request IA benefits from FEMA or whom FEMA may refer to its partners.

System: **DHS/S&T/PIA-026 Robotic Aircraft for Public Safety (RAPS)**

Component: **S&T**

Date of approval: **November 16, 2012**

S&T and the State of Oklahoma are partnering on the RAPS project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components. SUAS include small aircraft (typically under 55 pounds and having wingspans of 3-6 feet or less) that are operated using a

wireless ground control station. The aircraft are equipped with sensors and cameras that can capture images and transmit them to a ground control system to provide aerial views of emergency situations and situational awareness. S&T conducted a PIA to address the privacy impact of the system's surveillance and image capturing capabilities.

System: **DHS/USCG/PIA-001(b) Homeport Internet Portal**

Component: **USCG**

Date of approval: **November 16, 2012**

USCG currently uses the Homeport Internet Portal to provide secure information dissemination, advanced collaboration for Area Maritime Security Committees, electronic submission and approval for facility security plans, and complex electronic notification capabilities. Homeport includes a subsystem called the Alert Warning System (AWS), which provides USCG Headquarters, Districts, Sectors, and other units an enterprise solution for sending alerts and warnings to maritime security (MARSEC) partners, stakeholders, and appropriate port constituents for MARSEC level changes and other MARSEC-related activities requiring port-wide notifications. Through a Memorandum of Agreement between the USCG and the Transportation Security Administration (TSA), use of AWS capabilities will be shared between these two DHS components, thereby leveraging DHS investment in the system and avoiding duplicative operations and maintenance costs within DHS. The USCG issued this PIA update to include TSA operations center personnel as authorized users of Homeport's AWS, which contains non-sensitive PII and disseminates airport security information to authorized recipients.

System: **DHS/ICE/PIA-029 Alien Medical Records Systems**

Component: **ICE**

Date of approval: **November 27, 2012**

ICE maintains medical records on aliens that ICE detains for violations of U.S. immigration law. Aliens held in ICE custody in a facility staffed by the ICE Health Services Corps, a division of ICE's Office of Enforcement and Removal Operations, receive physical exams and treatment, dental services, and pharmacy services, depending on the alien's medical conditions and length of stay. To properly record the medical assessments and services, ICE operates the following information technology systems that maintain electronic medical record information: CaseTrakker, MedEZ, Dental X-Ray System, the Criminal Institution Pharmacy System, the Medical Payment Authorization Request Web System (MedPAR), and the Medical Classification Database. This PIA was originally published on July 25, 2011, and described the information in these medical record systems, the purposes for which this information was collected and used, and the safeguards ICE had implemented to mitigate the privacy and security risks to PII stored in these systems. The PIA was republished in full primarily to modify the description of the MedPAR system, which originally was to be hosted by the U.S. Department of Veterans Affairs, but now remains at ICE.

Date: February 13, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-04109 Filed 02/21/2013 at 8:45 am; Publication Date: 02/22/2013]