



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 DHS is making available eleven PIAs on various programs and systems in DHS. These assessments were approved and published on the Privacy Office's web site between December 1, 2011 and February 29, 2012.

DATES: The PIAs 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: Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, or email: pia@hq.dhs.gov.

SUPPLEMENTARY INFORMATION: Between December 1, 2011 and February 29, 2012 the Chief Privacy Officer of the DHS approved and published eleven Privacy Impact Assessments (PIAs) on the DHS Privacy Office web site, www.dhs.gov/privacy, under the link for "Privacy Impact Assessments." These PIAs cover eleven 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/USSS/PIA-007 Forensic Services Division (FSD) Polygraph System**

Component: **United States Secret Service (USSS)**

Date of approval: **December 15, 2011**

The FSD Polygraph Branch of the USSS uses the FSD Polygraph system to track all polygraph examinations that it administers. This database contains information on applicant and criminal polygraph examinations and their results. USSS is conducting this PIA because this system contains PII of individuals who undergo an exam.

System: **DHS/FEMA/PIA-019 Firehouse Database (Unclassified and Classified)**

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

Date of approval: **December 15, 2011**

The U.S. DHS FEMA Mount Weather Emergency Operations Center (MWEOC) Emergency Services Division (ESD) owns and operates two Firehouse Databases: 1) Firehouse Database (classified); and 2) Firehouse Database (unclassified). The difference between the two databases is that the classified Firehouse Database contains classified locations on which MWEOC ESD may respond at the MWEOC facility. FEMA uses the unclassified and classified Firehouse Databases to manage the collection, documentation, and reporting of information about emergency incidents, incident investigations, site inventory and inspections, staffing, scheduling, and personnel certifications and training of FEMA paramedics, emergency management technicians, firefighters, and other first responders at MWEOC ESD. FEMA is conducting this PIA because FEMA's unclassified and classified Firehouse Databases collects, uses, maintains, retrieves, and disseminates PII of MWEOC residents, employees and

contractors, visitors, as well as members of the immediate local community surrounding MWEOC. This PIA covers both the unclassified and classified Firehouse Databases.

System: **DHS/ALL/PIA-028(a) Freedom of Information Act (FOIA) and Privacy Act (PA) Records Program Update**

Component: **DHS**

Date of approval: **December 16, 2011**

The DHS Privacy Office is publishing an update to the current PIA, DHS/ALL/PIA-028, which outlines the risks presented by the use of PII in the various FOIA and PA processes and systems employed by DHS. This update introduces the use of a FOIA software application used for tracking FOIA requests.

System: **DHS/FEMA/PIA-020 Integrated Financial Management Information System (IFMIS) Merger**

Component: **FEMA**

Date of approval: **December 16, 2011**

The U.S. DHS FEMA's Office of the Chief Financial Officer owns and operates the IFMIS-Merger system. IFMIS-Merger is FEMA's official accounting and financial management system that pulls all financial data from other FEMA, DHS, and Government-wide systems (subsystems), and is the source of data for both internal and external financial reporting. The system records and tracks all financial transactions. FEMA is conducting this PIA because IFMIS-Merger collects uses, maintains, retrieves, and disseminates PII once pulled from the subsystems.

System: **DHS/S&T/PIA-012(a) Future Attribute Screening Technology (FAST)**
Passive Methods for Precision Behavioral Screening

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

Date of approval: **December 21, 2011**

The DHS Privacy Office is publishing an update to the current PIA, DHS/S&T/PIA-012 to increase the performance of FAST primary screening procedures and to increase the ability to differentiate malintent through the inclusion of passive stimuli. The FAST project, managed by the Human Factors/Behavioral Sciences Division (HFD), Homeland Security Advanced Research Projects Agency (HSARPA), S&T Directorate seeks to develop physiological and behavioral screening technologies that will enable security officials to test the effectiveness of current screening methods at evaluating suspicious behaviors and judging the implications of those behaviors. The FAST research is adding a new type of research, the Passive Methods for Precision Behavioral Screening (hereinafter FAST/Passive). The purpose of the FAST/Passive study is to build upon existing FAST research using volunteers and increase the performance of FAST primary screening procedures and to increase the ability to differentiate malintent through the inclusion of passive stimuli. The aim of the FAST/Passive study is to devise passive stimuli that will evoke malintent cues and incorporate these stimuli into the FAST screening project. The ultimate goal of the FAST screening project after the testing has been completed is to equip security officials with quantitative tools to rapidly assess potential and unknown threats.

System: **DHS/USSS/PIA-008 Secret Service Use of Advanced Imaging Technology (AIT)**

Component: **USSS**

Date of approval: **December 23, 2011**

USSS is deploying AIT, at Secret Service protective sites. This technology creates an image of the full body that highlights anomalies that are on the body. It is used as a secondary means of personnel screening at protected sites, and used after the primary screening measures indicate that an individual requires an additional level of screening.

To address privacy concerns associated with creating an image of an individual's body, the Secret Service employee who examines the image is at a remote location and cannot see the person who is being screened, only the image produced by the AIT. The Secret Service employee that is in the room with the person being imaged can communicate with the Secret Service employee who examines the image, but cannot view the image.

The image of the individual is not linked in any way to the individual nor does it they provide sufficient detail to be used for personal identification. The AIT does not have the capability to store, transmit, or print these images. In addition, an electronic privacy filter is applied to the remotely viewed image which renders the facial features unrecognizable.

System: **DHS/ALL/PIA-041 One DHS Overstay Vetting Pilot**

Component: **DHS**

Date of approval: **December 29, 2011**

DHS is conducting the One DHS Overstay Vetting Pilot to improve DHS' ability to identify and vet foreign nationals who have remained in the United States beyond their authorized period of admission (overstays). The pilot will attempt to streamline data sharing between the National Protection and Programs Directorate's United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement (ICE). The overstay vetting process is covered by existing PIAs for the CBP Automated Targeting System (ATS), US-VISIT Technical Reconciliation Analysis Classification System, and US-VISIT Arrival Departure Information System. In addition to this existing coverage, US-VISIT has worked with the DHS Privacy Office to complete this PIA specific to the Overstay Vetting Pilot to add another layer of analysis and transparency to this specific process which can be updated as the program matures. Data sharing conducted through this program allows DHS to better identify which individuals have overstayed their authorized periods of admission, and of those overstays, which are the highest law enforcement or national security priority for enforcement action by ICE. DHS is conducting this PIA because the pilot increases the sharing within DHS of PII about travelers.

System: **DHS/TSA/PIA-036 TSA Canine Website System (CWS)**

Component: **TSA**

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

Under the Aviation and Transportation Security Act, the TSA is responsible for security in all modes of transportation. TSA's National Explosives Detection Canine Team

Program (NEDCTP) prepares dogs and handlers to quickly locate and identify dangerous materials that may present a threat to transportation systems. The NEDCTP operates the CWS, which is a web-based system designed to assist in coordinating operations. The CWS is the central management database for all NEDCTP records and operations. The CWS collects PII to facilitate training, foster communication, and to perform administrative functions. 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 conduct a PIA.

System: **DHS/TSA/PIA-012 Transportation Worker Identification Credential Program**

Component: **TSA**

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

The TSA Directorate's TWIC system has undergone a PIA 3-Year Review. The PIA requires no changes and continues to accurately relate to its stated mission.

The TSA published a joint Final Rule with the United States Coast Guard to implement a 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 amended 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.

System: **DHS/ICE/PIA-032 FALCON Search & Analysis System (FALCON-SA)**

Component: **ICE**

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

U.S. ICE, a component agency within the DHS, is establishing a consolidated information management system called FALCON Search & Analysis System (hereafter, FALCON-SA). This system enables ICE law enforcement and homeland security personnel to search, analyze and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. ICE agents, criminal research specialists, and intelligence analysts use FALCON-SA to conduct research that support the production of law enforcement intelligence products, provide lead information for investigative inquiry and follow-up, assist in the conduct of ICE criminal and administrative investigations, assist in the disruption of terrorist or other criminal activity, and discover previously unknown connections among existing ICE investigations. ICE's use of the system is always predicated on homeland security, law enforcement, and intelligence activities. FALCON-SA is an internal system used only by ICE.

In order to mitigate privacy and security risks associated with the deployment of FALCON-SA, ICE has built technical safeguards into the system and developed a governance process that includes the operational components of ICE Homeland Security Investigations, the oversight functions of the ICE Privacy Office, Office Principal Legal Advisor, and Office of the Chief Information Officer.

This PIA is necessary because FALCON-SA accesses and stores PII retrieved from DHS, other government agency, and commercially available databases. It is also

necessary to provide public notice of the existence of FALCON-SA and to publicly document the privacy protections that are in place for the system.

System: **DHS/NPPD/PIA-022 Linking Encrypted Network system (LENS)**

Component: **NPPD**

Date of approval: **February 9, 2012**

DHS, NPPD, Critical Infrastructure Technology and Architecture (CITA) Project maintains the Linking Encrypted Network System (LENS), a data repository and application set that acts as a network of online portals or modules, allowing authorized users to obtain, post and exchange information and access common resources. NPPD conducted this PIA to examine the privacy impact associated with the collection of PII related to individuals who are LENS users or seeking access to LENS, as well as PII related to POCs that may be maintained within the LENS data repository. NPPD will conduct separate PIAs, as necessary, for those modules or applications residing on the LENS platform where the scope of the collection is beyond that of this PIA.

Date: March 12, 2012

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-6847 Filed 03/21/2012 at 8:45 am; Publication Date: 03/22/2012]