DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2013-0012]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security U.S. Immigration and Customs Enforcement - 014 Homeland Security Investigations Forensic Laboratory System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/U.S. Immigration and Customs Enforcement - 014 Homeland Security Investigations Forensic Laboratory System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0012 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

Instructions**:** All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket**:** For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Lyn Rahilly, Privacy Officer, (202-732-3300), U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, e-mail: ICEPrivacy@dhs.gov. For privacy issues please contact: Jonathan R. Cantor (202-343-1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

The Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "DHS/U.S. Immigration and Customs Enforcement (ICE) - 014 Homeland Security Investigations Forensic Laboratory (HSI-FL) System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

The Homeland Security Investigations Forensic Laboratory (HSI-FL) is an accredited crime laboratory located within ICE's Office of Homeland Security Investigations (HSI) that provides a broad range of forensic, intelligence, and investigative support services for ICE, DHS, and many other U.S. and foreign law enforcement agencies. Created in 1978 under the U.S. Department of Justice, Immigration and Naturalization Service, the HSI-FL became part of DHS on March 1, 2003, as part of the federal government's response to the 9/11 attacks. The HSI-FL is the only U.S. crime laboratory specializing in scientific authentication; forensic examination; research, analysis, and training related to travel and identity documents; latent and patent finger and palm prints; and audio and video files in support of law enforcement investigations and activities by DHS and other agencies. To facilitate forensic examinations and for use in forensic document training, research, and analysis, the HSI-FL maintains case files, a case management system, an electronic library of travel and identity documents (Imaged Documents and Exemplars Library (IDEAL)), and a hard copy library referred to as the HSI-FL Library.

As a crime laboratory specializing in the forensic examination and research of travel and identity documents, the HSI-FL attempts to determine the authenticity, authorship, and any actual or potential alterations of travel and identity documents. Examinations of such documents submitted by DHS and other U.S. and foreign law enforcement agencies and international organizations normally begin with a physical (naked eye, tactile) inspection and proceed to microscopic, instrumental, and comparative examinations, as necessary and appropriate. Depending on the document type, these examinations also may require the expert analyses of handwriting, hand printing,

typewriting, printing processes, papers, inks, and stamp impressions.

HSI-FL examinations are predominantly performed on documents used to establish identity or facilitate travel, such as passports, visas, identification cards, and border crossing cards, but can be performed on virtually any document, including envelopes, handwritten documents, letters, vital records, and typewritten documents. DHS and other federal, state, and international government agencies, or organizations such as the United Nations, may submit requests to HSI-FL for document authentication. In response, the HSI-FL may conduct an analysis and share the results of forensic examinations within DHS and externally with other government agencies and international organizations in the course of law enforcement investigations and for admission into evidence in judicial proceedings.

In addition to the forensic examination of documents, the HSI-FL performs fingerprint analysis. The fingerprint analysis performed by HSI-FL may not be document-related. This analysis may include fingerprints collected from evidence during an investigation such as firearms, drug packaging, currency, periodicals, photo albums, CDs and computers. Fingerprint analysis will include both latent (invisible to the naked eye) and patent (visible to the naked eye) finger and palm prints.

The HSI-FL also performs technical enhancements of audio and video files. The audio and video work performed by the HSI-FL is limited to enhancing files to improve their quality and clarifying detail to allow law enforcement agencies to better examine the files. For example, this could include removing background noise from an audio file or improving the clarity of an image in a video. The HSI-FL is not responsible for performing forensic examinations of the audio or video files but merely performs

technical work to permit law enforcement agencies outside of the HSI-FL to conduct law enforcement investigations.

Laboratory Information Management System

In order to track evidence and cases, the HSI-FL implemented the Laboratory Information Management System (LIMS) as their case management system. LIMS allows the HSI-FL to capture information about the individual submitting the request for analysis, identify the evidence submitted, track the evidence as it moves throughout the HSI-FL for chain of custody purposes, capture case notes and results of examinations, store electronic images of evidence, and produce reports of findings. LIMS also captures other case-related activities such as descriptions of expert witness testimony provided by HSI-FL employees.

The HSI-FL also uses LIMS to record and store operational (non-forensic) requests for assistance, hours HSI-FL staff spend on training activities, and digital copies of training certificates of completion. In addition, LIMS generates recurring and *ad hoc* statistics reports in support of HSI-FL staff operations and management request.

Imaged Documents and Exemplars Library

The IDEAL database and the HSI-FL Library contain two categories of records: (1) travel and identity documents and (2) reference materials used to help in the forensic analysis of travel and identity documents. The HSI-FL maintains the documents and reference materials in both hard copy and electronic format for use in comparative forensic examination and fraudulent document training, research, and analysis. The hard copies are maintained in the HSI-FL Library while the electronic copies are stored in the IDEAL database. IDEAL contains electronic images and document characteristics for all

documents and reference materials stored in the HSI-FL Library and allows HSI-FL employees to access these electronic images and document characteristics from their own workstations. Further, IDEAL provides the inventory control of the hard copy material in the HSI-FL Library, which includes the support of "checking out" hard copy documents and reference materials in the HSI-FL Library by HSI-FL employees.

IDEAL indexes and assigns to all documents added to the HSI-FL Library an IDEAL identification number (IDEAL ID Number) and bar code, thus providing a standard identification and tracking mechanism and permitting indexing. The IDEAL ID Number is system-generated and allows documents to be quickly located in IDEAL. The bar code number links the images maintained in IDEAL to hardcopies maintained in the HSI-FL Library.

The HSI-FL collects and maintains genuine, altered, and counterfeit travel and identity documents (hereafter, "documents") in hard copy format from international organizations, government agencies, and law enforcement organizations from across the United States and around the world to research methods of document production and authenticate questionable documents through comparative forensic examinations. These travel and identity documents include documents such as passports, identification cards, birth certificates, stamps, visas, and any other document that can be used to establish nationality or identity from any country including the United States.

From these same sources, the HSI-FL also collects information that helps with the identification of potential counterfeit characteristics, potential fraud, security features, and other information valuable to forensic analysis (hereafter, "reference materials"). HSI-FL employees also make use of reference materials issued by the United States and

other nations that contain useful information such as descriptions of security features of travel and identity documents or information concerning attempts to counterfeit or alter such documents.

Document characteristics including personally identifiable information (PII) are manually entered into IDEAL to catalogue, track, and facilitate searching for documents and reference materials. Depending on the particular document, the document characteristics entered into IDEAL may include the document type, document number (e.g., passport number, driver's license number, state identification number), country of origin, region, authenticity of the document, information regarding the location and availability of the hard copy document in the HSI-FL Library, and a short description of the document. Social Security Numbers are not directly entered into IDEAL, instead the serial number on the back of the document is entered into the system. In addition to manually entered information, the document is scanned into IDEAL capturing and storing additional information, including PII. The PII stored on the images is view-only and may not be searched or used in any other manner in IDEAL.

The HSI-FL divides the documents maintained in the HSI-FL Library and electronically in IDEAL into five different categories: (1) genuine standard documents; (2) verified documents; (3) unverified documents; (4) counterfeit documents; and (5) altered documents. The first category, genuine standard documents, is comprised of documents never used in circulation and officially submitted to the HSI-FL by a valid issuing authority or other officially recognized domestic or foreign agency. Valid issuing authorities produce genuine standard documents as samples of particular travel and identity documents (e.g., passports) and include all of the same characteristics and

security features of that document. Genuine standard documents are usually issued under an obviously fictitious name, such as "Happy Traveler," to ensure they are easily identified as samples. Genuine standard documents do not contain the PII of actual individuals; however, they may contain photographs of individuals who have consented for their images to be used and distributed on these sample documents. The HSI-FL uses genuine standard documents during forensic analysis to authenticate other travel and identity documents purporting to have been issued by the same issuing authority. This authentication is used to support law enforcement investigations in response to government agency inquiries from the United States and around the world and judicial proceedings.

The remaining four categories of documents are provided to the HSI-FL by the valid issuing authority of a domestic or foreign agency, or from other sources including international organizations; DHS; the U.S. Department of State (DOS); and other federal, state, and foreign government agencies and law enforcement organizations. These four categories of documents may be directly provided for inclusion in the HSI-FL Library or may be initially provided for other purposes such as forensic examination and then retained by the HSI-FL, with the submitting agency's permission, after the examination is complete. The HSI-FL determines whether to include specific documents in the HSI-FL Library based upon the HSI-FL Library's need for that document, particularly whether the HSI-FL Library currently has a document of that type already in the HSI-FL Library. These categories of documents may contain the PII of individuals. Verified documents are documents that the HSI-FL has found to conform to comparable genuine travel and identity documents. Unverified documents are documents that the HSI-FL has analyzed

and has not conclusively determined are verified, counterfeit, or altered. Counterfeit documents are documents that the HSI-FL has determined through forensic analysis are not authentic documents issued by a foreign or domestic governmental issuing authority. Altered documents are documents that were originally authentic documents issued by a foreign or domestic governmental issuing authority that have been changed in an unauthorized manner.

Certain designated users at DOS have read-only access to IDEAL. This read-only access allows certain designated DOS employees to search and view travel and identity documents and reference materials. These documents and materials may contain the PII of actual individuals. This information is used by the DOS for their reference and in support of their mission. This use includes supporting the processing of petitions or applications for benefits under the Immigration and Nationality Act, and other immigration and nationality laws including treaties and reciprocal agreements. It also includes when the DOS requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications. Authorized users from the DOS are the only non-DHS users with direct access to IDEAL.

Consistent with DHS' information sharing mission, information stored in the DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate

federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the system of records notice.

This proposed rulemaking will be included in DHS' inventory of record systems.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ ICE-014 Homeland Security Investigations Forensic Laboratory System of Records. Some information in DHS/ ICE-014 Homeland Security Investigations Forensic Laboratory System of Records relates to official DHS national security, law enforcement, immigration, and intelligence activities. These exemptions are needed to

protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS' ability to obtain information from third parties and other sources; and to protect the privacy of third parties. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A system of records notice for DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for Part 5 continues to read as follows:

Authority: 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add at the end of Appendix C to Part 5, the following new paragraph 70:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

70. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records contains records of evidence and cases submitted to the HSI-FL. This information will include information on the individual submitting the request, identify the evidence submitted, track the evidence as it moves throughout the HSI-FL, capture case notes and results of examinations, store electronic images of evidence, and produce reports of findings. Other case-related records are maintained including descriptions of expert witness testimony provided by HSI-FL employees. Records in the DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records also include the library of genuine, altered, and counterfeit travel and identity documents provided to the HSI-FL by international organizations, government agencies, and law enforcement organizations from across the United States and around the world to research methods of document production and authenticate questioned documents through comparative forensic examinations. The DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from

the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that

investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose classified and other security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: April 22, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-11727 Filed 05/15/2013 at 8:45 am; Publication Date: 05/16/2013]