9111-28

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2013-0078]

Privacy Act of 1974; 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 Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, "Department of Homeland Security/U.S. Immigration and Customs Enforcement - 014 Homeland Security Investigations Forensic Laboratory System of Records." This system of records allows the Department of Homeland Security/U.S. Immigration and Customs Enforcement to collect and maintain records by the Homeland Security Investigations Forensic Laboratory (HSI-FL). The HSI-FL is a 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), and a hard copy library referred to as the HSI-FL Library. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking elsewhere in the Federal Register to exempt this system of records from certain provisions of the Privacy Act. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0078 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 rulemaking. 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, please visit 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 questions, 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

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) proposes to establish a new DHS system of records titled, "DHS/ICE-014 - Homeland Security Investigations Forensic Laboratory System of Records."

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 hard copies 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 the 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 this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this

system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established system 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.

Below is the description of the DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)-014

System name:

DHS/ICE-014 Homeland Security Investigations Forensic Laboratory (HSI-FL)

Security classification:

Law enforcement sensitive.

System location:

Records are maintained at U.S. Immigration and Customs Enforcement Headquarters in Washington, DC and in field offices, and electronic records are maintained in LIMS, IDEAL, and other IT systems.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

1. Individuals whose information is contained on United States or international travel and identity documents, such as driver's licenses, passports, and other forms of identification, that are maintained in the Homeland Security Investigations Forensic Laboratory (HSI-FL) Library;

2. Individuals whose information is contained on United States or international travel and identity documents, such as driver's licenses, passports, and other forms of identification, that are provided to the HSI-FL for forensic examination during a criminal or administrative law enforcement investigation;

3. Individuals who are the subjects of current or previous law enforcement investigations by other domestic or foreign agencies where the HSI-FL is providing support and assistance;

4. Individuals who are the subjects of current or previous law enforcement investigations into violations of U.S. customs and immigration laws, as well as other laws

and regulations within ICE's jurisdiction, including investigations led by other domestic or foreign agencies, where the HSI-FL is providing support and assistance; and

5. Individuals whose image or voice may be captured on video or audio files where the HSI-FL is provided the file to perform technical enhancements of the file.

Categories of records in the system:

Categories of records in this system include:

1. Biographic, descriptive, historical and other identifying data, including: names; photographs; fingerprint identification number; date and place of birth; passport and other travel document information; nationality; aliases; Alien Registration Number (A–Number); Social Security Number; other identification numbers, contact or location information (e.g., known or possible addresses, phone numbers); visa information; employment, educational, immigration, and criminal history; height, weight, eye color, hair color and other unique physical characteristics (e.g., scars and tattoos).

2. Fingerprints or palm prints of individuals whose information is provided to the HSI-FL for forensic examination.

3. Case-related data, including: Case number, record number, and other data describing an event involving alleged violations of criminal or immigration law (such as, location, date, time, event category (event categories describe broad categories of criminal law enforcement, such as immigration worksite enforcement, contraband smuggling, and human trafficking)); types of criminal or immigration law violations alleged; types of property involved; use of violence, weapons, or assault against DHS personnel or third parties; attempted escape; and other related information. ICE case

management information, including: case category; case agent; date initiated; and date completed.

4. Birth, marriage, education, employment, travel, and other information derived from affidavits, certificates, manifests, and other documents presented to or collected by ICE during immigration and law enforcement proceedings or activities. This data typically pertains to subjects, relatives, and witnesses.

5. Data concerning personnel of other agencies that arrested, or assisted or participated in the arrest or investigation of, or are maintaining custody of an individual whose arrest record is contained in this system of records. This can include: name; title; agency name; address; telephone number; and other information.

Authority for maintenance of the system:

8 U.S.C. 1103, 44 U.S.C. 3101, 18 U.S.C. 496, 18 U.S.C. 911, 18 U.S.C. 1001, 18 U.S.C. 1028, 18 U.S.C. 1425, 18 U.S.C. 1426, 18 U.S.C. 1427, 18 U.S.C. 1541, 18 U.S.C. 1543, and 18 U.S.C. 1546.

Purpose(s):

The purposes of this system are to:

1. Maintain records related to the scientific authentication, examination, research, and analysis of travel and identity documents, fingerprints, and palm prints in accordance with established laboratory policies and procedures, scientific principles, and accreditation standards.

2. Maintain a library of travel and identity documents and associated reference materials for use in forensic examinations, investigations, training, and other activities.

3. Support the forensic examinations on a full range of documents, including but not limited to, passports, visas, driver's licenses, identification cards, border crossing cards, handwritten documents, vital records, and typewritten documents. The analysis may include, but is not limited to, an examination of handwriting, hand printing, typewriting, printing processes, security features, papers, inks, and stamp impressions.

4. Maintain records facilitating the preparation of written laboratory reports and delivery of expert witness testimony in both legal proceedings.

5. Support the provision of training in fraudulent document detection, creation of document intelligence alerts and reference guides, and provision of direct assistance to federal, state and local agencies, as well as foreign governments and commercial entities to combat document fraud.

6. Provide assistance within ICE and to domestic and foreign agencies to support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of law.

7. To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ) (including U.S. Attorneys' Offices) or

other federal agency conducting litigation or proceedings before any court, adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property

interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. When a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure, a disclosure may be made to federal, state, local, tribal, territorial, international, or foreign law enforcement agencies or other appropriate authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order.

H. To courts, magistrates, administrative tribunals, opposing counsel, parties, and witnesses, in the course of immigration, civil, or criminal proceedings (including discovery, presentation of evidence, and settlement negotiations) when DHS determines

that such disclosure is relevant and necessary to the litigation and one of the following is party to the proceedings or has an interest in such proceeding:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity where the government has agreed to represent the employee; or

4. The United States, where DHS determines that litigation is likely to affect DHS or any of its components.

I. To federal, state, local, tribal, territorial, or foreign government agencies, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates or to elicit information required by DHS to carry out its functions and statutory mandates.

J. To federal, state, local, tribal, or territorial government agencies seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

K. To federal, state, local, tribal, or territorial government agencies, or other entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of national security, intelligence, counterintelligence, or antiterrorism

activities authorized by U.S. law, Executive Order, or other applicable national security directive.

L. To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

M. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

N. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such disclosure is to support the conduct of national intelligence and security investigations or to assist in anti-terrorism efforts.

O. To federal, state, local, tribal, territorial, or foreign government agencies or entities or multinational government agencies when DHS desires to exchange relevant data for the purpose of developing, testing, or implementing new software or technology whose purpose is related to this system of records.

P. To federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to

ensure the safety of law enforcement officers who may be working on related law enforcement matters.

Q. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements; or when the Department of State 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.

R. To the Department of State to provide read-only access of records maintained in the Imaged Documents and Exemplars Library to assist the Department of State with their validation of travel and identity documents.

S. To federal, state, local, tribal, territorial, or foreign government agencies for purposes of completing and providing results of requested forensic examinations to the requesting agency.

T. To the Department of Justice (including United States Attorneys' Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when necessary to assist in the development of such agency's legal and/or policy position.

U. To the U.S. Senate Committee on the Judiciary or the U.S. House of Representatives Committee on the Judiciary when necessary to inform members of Congress about an alien who is being considered for private immigration relief.

V. To federal, state, tribal, territorial, local, international, or foreign government agencies or entities for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) to verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) to verify the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

W. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored in hard copy and electronically on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

Records may be retrieved by name, identification numbers including case or record number if applicable; other personal identification numbers including Alien Registration Number (A–Number), fingerprint identification number, and other personal identification numbers; and case related data and/or combination of other personal identifiers including, but not limited to, date of birth and nationality.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

After the forensic examination is completed, all case files shall be stored as closed case files onsite at HSI-FL for 6 years followed by 10 years in offsite temporary storage for a total of 16 years. Exception: All war crimes and capital cases shall be held indefinitely onsite at the HSI-FL.

System Manager and address:

U.S. Immigration and Customs Enforcement, Homeland Security Investigations Forensic Laboratory, Unit Chief, 8000 West Park Drive, McLean, VA 22102-3105.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/ICE will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to ICE's FOIA Officer, whose contact information can be found at http:// www.dhs.gov/foia under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;

- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records in the system are supplied by several sources. In general, information is obtained from federal, state, local, tribal, or foreign governments. More specifically, DHS/ICE–014 records are derived from the following sources: (a) other federal, state, local, tribal, or foreign governments and government information systems; and (b) evidence, contraband, and other seized material.

Exemptions claimed for the system:

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 in accordance with this rule.

Dated: April 22, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-11722 Filed 05/15/2013 at 8:45 am; Publication Date: 05/16/2013]