Privacy Impact Assessment
for the

Laboratory Information Management System

DHS/ICE/PIA-046

December 15, 2016

Contact Point
Peter Edge
Executive Associate Director
Office of Homeland Security Investigations
U.S. Immigration and Customs Enforcement
202-732-5100

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Office of Homeland Security Investigations (HSI), a directorate within U.S. Immigration and Customs Enforcement (ICE) of the Department of Homeland Security (DHS), owns and operates the Laboratory Information Management System (LIMS) as part of its Forensic Laboratory (HSI-FL). LIMS is a case management system that allows ICE employees at the HSI-FL to capture information about requests for forensic analysis or technical enhancements; identify the evidence submitted; track that evidence as it moves throughout the HSI-FL for chain of custody purposes; capture case notes and results of forensic examinations; document technical enhancements performed; store electronic images of evidence; and produce forensic reports of findings (forensic reports) or non-forensic reports of technical enhancements made to audio-visual (AV) materials. ICE implemented LIMS to facilitate and store data, including personally identifiable information (PII), related to the scientific authentication, examination, research, and analysis of documents, and finger and palm prints performed to determine authenticity, authorship, and actual or potential alterations. The system also stores data related to the technical enhancements made to AV materials by HSI-FL staff and HSI-FL operational and training data.

Overview

The HSI-FL is an accredited crime laboratory that supports law enforcement investigations conducted by federal, state, local, and international law enforcement agencies. The laboratory specializes in the scientific authentication and forensic examination of travel and identity documents, as well as the identification of latent finger and palm prints. The HSI-FL also conducts the technical enhancement of AV materials. In addition, HSI-FL conducts research, analysis, and training in these areas.

The HSI-FL Questioned Document Section performs forensic examinations of travel and identity documents for the purpose of determining authenticity and any alterations of original documents. These examinations require the analyses of handwriting, hand printing, typewriting, printing processes, papers, inks, and stamp impressions. Commonly examined documents include passports, visas, identification cards, and border crossing cards, but forensic examinations can be performed on virtually any document, including envelopes, handwritten documents, letters, vital records, and typewritten documents.

The HSI-FL Latent Print Section provides finger and palm print services that support law enforcement investigations. These services include the processing and examination of latent prints, latent print comparison, inked print comparison, and searches for finger and palm print matches in federal print databases. Examiners process latent finger and palm prints on firearms, drug packaging, currency, periodicals, photo albums, CDs, and computers. Results from these

examinations are provided to the investigators and may be used in the course of law enforcement investigations and could be admitted into evidence in judicial proceedings.

HSI-FL personnel also perform technical enhancements of AV materials. The AV work performed at the HSI-FL is limited to enhancing materials to improve their quality and clarifying details, allowing law enforcement agencies to better examine the materials. Examples of the type of AV enhancement performed include removing background noise from an audio file or improving the clarity of an image in a video. The enhancement services provided by the HSI-FL are solely for the purpose of providing investigative leads and support to law enforcement agents in the field. Unlike forensic services conducted at the HSI-FL, which offer opinion-based assessments of evidence, the interpretation of the enhanced AV materials are solely the responsibility of the submitting investigator.

LIMS

As a crime laboratory, the HSI-FL is accredited by the American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD/LAB). In order to achieve and maintain ASCLD/LAB-*International* accreditation, the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) International Standard 17025:2005 and ASCLD/LAB-*International* Supplemental Requirements for Testing Laboratories (2011) accreditation requirements are followed at the laboratory.[1] These requirements mandate that a crime laboratory be able to accurately track cases and chain of custody for evidence within a laboratory environment. The HSI-FL purchased LIMS to track evidence and cases, and to comply with the ASCLD/LAB accreditation requirements. LIMS is a commercial off-the-shelf product customized to meet HSI-FL requirements. Only HSI-FL staff has access to the LIMS system. LIMS allows the HSI-FL staff to capture information about individuals submitting requests for HSI-FL services, identify evidence submitted, track that evidence as it moves throughout the HSI-FL, capture case notes, and store the results of examinations and electronic images of evidence. LIMS captures other case-related activities such as descriptions of expert witness testimony provided by HSI-FL examiners and it generates reports.

LIMS stores requests by HSI-FL customers for status updates on forensic examinations and general case-related inquiries. The LIMS training module maintains information concerning HSI-FL staff training activities and digital copies of employee training certificates. LIMS generates recurring and ad-hoc statistical reports in support of HSI-FL staff operations and management requests. The system tracks and manages case information enabling the HSI-FL staff to support the tracking and sharing of information about questioned documents and/or print examinations.

[1] ASCLD/LAB-International Supplemental Requirements (Testing) 2011 Edition.

Information Collection and Privacy and Data Integrity Controls

During the course of a law enforcement investigation, an investigator may send a request to the HSI-FL for the forensic examination of evidence. Travel and identity documents may be submitted to the HSI-FL to determine authenticity and the presence of alterations. The laboratory performs detailed and complex examinations of latent and inked impressions from evidence to the known impressions of subjects or searched within the DHS's Office of Biometric Identity Management's Automated Biometric Identification System (IDENT),[2] the Federal Bureau of Investigation's Next Generation Identification (NGI) System,[3] or the Department of Defense's Automated Biometric Identification System (ABIS). [4] The HSI-FL also provides enhancement services for audio and visual (AV) media (e.g., remove background noise, enhance picture quality).

Upon arrival at the HSI-FL, a seized property specialist receives the evidence and creates a case in LIMS. The seized property specialist enters the following data:

- Information identifying the requesting agency representative;
- Identification information used by the requesting agency such as a case number;
- Name of the HSI-FL examiner assigned to the case; and
- An initial description of the evidence submitted for examination.

LIMS then automatically generates a unique HSI-FL case record number for the new case. As the case is worked at the HSI-FL, LIMS automatically records each staff member's activities in the system. This capturing of the access and use of case data supports auditing and accountability as well as the privacy, security, quality, and integrity of PII in LIMS.

Once LIMS generates the case record number, the seized property specialist assigns the case to an HSI-FL examiner and stores the evidence in the HSI-FL secure evidence room. The HSI-FL examiner is notified of the case assignment upon accessing LIMS. The HSI-FL examiner obtains custody of the case evidence and then proceeds with the forensic examination. During this initial forensic examination the HSI-FL examiner creates a more comprehensive description of the evidence in LIMS as a means of uniquely identifying it. In the case of travel and identity documents that may be counterfeit, this description may contain real or fictitious PII (e.g., passport names,

---

[2] *See* DHS/USVISIT-001 DHS Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

[3] *See* JUSTICE/FBI Next Generation Identification PIA, *available at* https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files and JUSTICE/FBI-009. *See* Fingerprint Identification Records System SORN, *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-01-25/pdf/E7-1176.pdf.

[4] *See* ABIS – Army CIO/G-6 PIA, *available at* http://ciog6.army.mil/Portals/1/PIA/2015/DoD%20ABIS.pdf and A0025-2 PMG (DFBA) DoD – Defense Biometric Identification Records SORN, *available at* http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/581425/a0025-2-pmg-dfba-dod.aspx.

numbers). HSI-FL has the capacity to conduct searches using this PII, but will only search using PII to determine whether a case was received, worked, or returned when the submitter has no other case information and the case cannot otherwise be located.

When questioned travel and identity documents are submitted as evidence to the HSI-FL for forensic examination, images of the questioned documents are electronically stored in LIMS. The documents are compared to genuine standards on file in the HSI-FL Reference Library, a collection of sample travel and identification documents. The results of the comparative examination are entered into LIMS by the examiner.

When an investigator submits evidence to the HSI-FL for latent print processing, the HSI-FL develops latent prints using processes that render the prints visible. The examiner photographs developed latent prints and saves them to a CD that is retained in the case jacket and stored with the physical file. The latent print images are not stored in LIMS.[5]

The examiner conducts the examination of the fingerprint and enters the results of the examination into LIMS. If the fingerprint is from an unknown individual and identification is requested, the examiner may also query the fingerprint in IDENT, NGI, and ABIS. If a palm print is submitted for examination, it can be queried in the NGI system. The query and any positive identification of the owner of the print are entered into LIMS in the form of case notes.

Investigative agencies may submit audio and video AV materials to the HSI-FL to enhance their quality and clarify details (e.g., remove background noise, enhance picture quality) to allow the submitting agency to better examine the materials and develop investigative leads. AV materials do not undergo forensic examination. AV memoranda identify the enhancements made to the AV materials and do not contain forensic findings. The original AV materials are always returned to the submitter after the technical enhancements are completed. The HSI-FL maintains copies of the AV materials that were enhanced, as well as the memoranda.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Pursuant to the Homeland Security Act of 2002 (P.L.107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in titles 8, 18, 19, 21, 22, 31, and 50 of

[5] A back-up copy of the CD is also made in case there is damage or corruption of the primary CD. The back-up copy is placed in a sealed derived evidence envelope and it is also filed in the case jacket and stored with the physical case file. Both the primary and back-up copy CDs are retained and destroyed in accordance with the retention schedule for hard-copy files.

the U.S. Code. The Secretary delegated this authority to ICE in DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Homeland Security Investigations Forensic Laboratory,[6] which covers forensic examinations, records, and procedures in accordance with established laboratory policies, scientific principles, and accreditation standards.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The system received an Authority to Operate (ATO) on August 27, 2010, for a period of three years. LIMS is now operating under the new DHS Ongoing Authorization (OA) process that provides Continuous Monitoring of the security posture of the system.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. ICE is developing a records retention schedule for these records. Records are being retained for five years, unless they involve potential war crimes.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This system does not collect information from the public. Information is collected from law enforcement agencies or individuals representing those agencies, therefore LIMS is not subject to the requirements of the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

[6] *See* DHS/ICE-014 Homeland Security Investigations Forensic Laboratory, 81 FR 45523 (July 14, 2016).

2.1 Identify the information the project collects, uses, disseminates, or maintains.

LIMS maintains the following categories of information:

Submitter Information: Information about individuals representing federal, state, local, and international law enforcement and government agencies submitting evidence or requests for assistance[7] to the HSI-FL.

- For Individuals: Name, title, department, agency, office, address, phone numbers, and email address.
- For Entities: Name, address, and phone number.

Case Information: LIMS captures four types of case information along with the type of examination requested. These are: type of case (criminal or non-criminal), whether the subject is in custody, whether another laboratory has previously examined the case, and case identifiers. Case identifiers are the identifying numbers and, when applicable, operation name that uniquely identifies a case.

HSI-FL receives requests for examinations from federal, state, and international law enforcement agencies and collects the respective case identifying numbers. The following types of numbers may be entered into LIMS as case identifiers: agency case number, FBI identification number, State ID Number, Incident Number (ICE and U.S. Customs and Border Protection (CBP) only), Chain of Custody Serial Number, Alien Registration Number (A-Number), and Related HSI-FL Case Number. HSI-FL also generates a unique case number for each new case using LIMS.

Finger/Palm Print Results: Results of queries of federal biometric databases (IDENT, NGI, and ABIS). Database searches yielding negative results return no further information. Database searches yielding positive results may return the print owner's name, date of birth, and associated database number, and the date the prints were taken. Queries resulting in positive identifications will be entered into LIMS as case notes. Information that may be included in these case notes includes the owner's name and date of birth, and the date the print was taken.

Evidence Descriptions and Reports: This includes descriptions of evidence, forensic reports, and non-forensic AV reports detailing technical enhancements made to AV materials. Both descriptions and reports in LIMS may contain genuine and fictitious information that is recorded from the documents submitted for examination. This information may relate to U.S.

[7] Requests for assistance may be returned without examination if the submission is not made in accordance with established HSI-FL procedures (i.e., improper labeling or packaging of evidence, incomplete or inaccurate descriptions of evidence, evidence not suitable for examination).

citizens, residents, and aliens. Specifically, the following data are entered into LIMS under this category:

- Type of evidence submitted (e.g., passport, visa, firearm, birth certificate, drug wrapping, AV materials);
- Images of the evidence submitted, which may contain PII such as name, photograph, identification numbers, address, and other information unique to the type of evidence being examined;
- Description of the evidence submitted to the HSI-FL including identifying information. This could include name, date of birth, race, sex, Social Security number (SSN), A-Number, FBI identification number, or any other information that is present on documentary evidence;
- Forensic reports, which may contain images of the evidence, a description, findings, and supporting information. For fingerprint or palm print examinations, the reports will also describe the print databases queried (i.e., IDENT, NGI, ABIS) and any examiner-identified positive matches from the print databases or a statement as to whether or not the unidentified prints have been entered into the unsolved files of each of the queried databases; and
- Non-forensic reports of enhancements made to AV materials.

Audio and Video (AV) Materials

The information stored in LIMS regarding enhancements made to AV materials is limited to submitter information, minimal case identification information (i.e., type of case, whether the subject is in custody, whether another laboratory has previously examined the case, and case identifiers), a general description of the evidence, and a report describing the enhancements made to the evidence. AV materials are not stored in LIMS but returned to the submitter upon completion of the enhancement.

2.2 What are the sources of the information and how is the information collected for the project?

HSI offices and other federal, state, and local law enforcement agencies submit requests for examination along with travel and identity documents, finger and palm prints, and AV materials to HSI-FL during the course of law enforcement investigations. Requests for assistance and items for examination are shipped, physically delivered, or sent electronically via encrypted email from federal, state, and international law enforcement agencies[8] to the HSI-FL, depending

[8] Submitters complete ICE Form 73-0003, Request for Laboratory Examination, documenting submitter information, case information, and types of examinations requested.

on the nature of the item. When a latent print examiner identifies a strong possible print match in a federal print database, the examiner requests and downloads a finger/palm print card from the database owner. The print card, which is used for closer examination and comparison, contains the name of the print's owner, an identification number, and images of finger/palm prints.[9]

Submitter Information in LIMS is obtained from the request for examination form completed by the law enforcement agency that has requested HSI-FL assistance with a forensic examination or AV enhancement. HSI-FL receives this information along with the evidence for examination via tracked mail and courier services, through physical delivery by a representative of the submitting agency, or using encrypted email.

Case Information is obtained from the request for examination form completed by the law enforcement agency that has requested HSI-FL assistance with a forensic examination or AV enhancement. HSI-FL also generates a unique case number for each new case using LIMS.

Finger/Palm Print Results are obtained from the federal fingerprint databases queried by HSI-FL during an examination. These databases are the FBI's NGI, DHS's IDENT, and DOD's ABIS. HSI-FL staff collect this information by logging in to each of these systems and uploading the fingerprint or palm print data for matching against identified prints in the system. Examiners then compare system generated hits to the known fingerprint card of the suspected hit. If an identification is suspected, the HSI-FL will request a finger/palm print card from the database owner and download it directly from the system. If the examiner determines that the two prints are a positive match, the print card containing a name, set of prints, and an identifying number will be identified as a match and saved in LIMS as part of the case. No prints or records of possible hits are retained if there is not a positive match.

Evidence Descriptions and Reports in LIMS are obtained from various sources. Images of the evidence are often taken during the intake process at the HSI-FL, and uploaded into LIMS. Latent prints present on evidence are processed and photographed by HSI-FL staff, but the photographs of prints are not loaded into LIMS. During the forensic examinations of documents or other items, the HSI-FL examiners enter a description of the evidence in LIMS that identifies the unique details of the evidence and which may contain both genuine and fictitious information.

The examiners also query the HSI-FL database called Imaged Documents and Exemplars Library (IDEAL)[10] to obtain information that helps them determine if an identity document is genuine or counterfeit. IDEAL is a centralized repository of travel and identity documents and reference material used to help in the forensic analysis of travel documents. IDEAL captures document specifications submitted from the authority that produced the document.

[9] The finger/palm print card includes fingerprints, a name, and an identification number. Palm prints may be provided together or separately from fingerprints on cards.
[10] *See* DHS/ICE/PIA-035 Imaged Documents and Exemplars Library (IDEAL), *available at* www.dhs.gov/privacy.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

Trained seized property specialists at the HSI-FL maintain and inventory documents, finger/palm prints, and AV materials submitted to the HSI-FL. The LIMS Program Manager conducts a physical inventory of evidence received by the laboratory for analyses twice a year. At that time, the Program Manager compares the data entered into LIMS with the physical records the HSI-FL also maintains on the cases to identify discrepancies or inaccuracies. The Information System Security Officer (ISSO) for LIMS performs weekly reviews of the system audit logs to ensure no evidence records were altered during the period of review. Any error is reported to the LIMS Program Manager and the HSI-FL Laboratory Director for investigation.

Trained, authorized HSI-FL staff members enter the data into LIMS during the course of their forensic examinations or AV enhancements. The completed results of initial forensic examinations are reviewed by a secondary examiner and then by a supervisor. Any inconsistencies found by the secondary examiner are brought to the attention of the initial examiner to resolve. If there is not agreement between the two examiners the matter moves to a supervisor to resolve prior to the finalization of the case. Finally, the supervisor performs an administrative review of the case, which involves reviewing the results of evidence and checking for accuracy to ensure policy and procedures were followed. Upon completion of the secondary examination, the administrative review is marked as completed in LIMS.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: LIMS captures the PII present on evidence submitted for examination. This PII may be that of individuals who are not suspected of unlawful activities but whose data appears on the evidence. LIMS also captures case identifier numbers submitted by law enforcement agencies that may link to subjects of investigations. There is a risk that these individuals will be harmed by association with a criminal investigation or that they will be improperly identified as a person under investigation or suspicion.

Mitigation: The HSI-FL uses PII present on evidence solely for descriptive purposes, to uniquely identify evidence submitted for examination or enhancement. No assessment is made of the guilt or innocence of an individual whose PII is present on examined evidence or whose information may be linked to a case identifier number.

Case identifier numbers that may link to subjects of investigations are included in LIMS only when provided by submitting law enforcement agencies. Their inclusion in LIMS is solely as a mechanism for case identification, allowing for the efficient and complete tracking and retrieval of information relating to a case submitted for examination.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Submitter information is used to keep track of the agencies and representatives of those agencies that have submitted evidence for examination. This information is required to identify the submitting agencies, facilitate correspondence with those agencies during the examination process, and to notify them when final reports have been completed.

Case Information is used to uniquely identify cases in LIMS and to allow for linking, searching, and retrieving case materials (i.e., evidence, case notes, images, descriptions of evidence, and forensic and non-forensic reports). This enables accurate and complete retrieval of all case materials submitted to or generated by the HSI-FL. Case Information may also be used to connect and retrieve related cases within LIMS.

Evidence Descriptions and Reports are used to identify evidence and document findings of forensic examinations and technical enhancements. They also serve as a record of the work performed by HSI-FL. Examiners review case information and reports to prepare their testimony for legal proceedings. The HSI-FL's collection of PII that is part of the evidence submitted for examination, such as identity documents, is incidental. The HSI-FL does not use the PII in any way outside of the forensic examination or technical enhancement process. Examiners draft and store the forensic and non-forensic reports in LIMS.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that evidence submitted to the HSI-FL contains PII, such as names on identity documents, that is incidental to the HSI-FL's purpose in obtaining these materials, i.e., to conduct forensic examinations or technical enhancements. This creates a risk that the HSI-FL is over-collecting PII and putting it at unnecessary risk.

Mitigation: ICE considered this risk and determined the PII collection cannot be minimized without compromising the integrity and effectiveness of the HSI-FL's forensic examinations and technical enhancements. The HSI-FL's sole reason for collecting evidence and AV materials is to conduct forensic examinations and technical enhancements. The PII that may be included on the evidence or in the AV materials is not in and of itself important to the examiner. Whether a travel document displays the name "John Smith" or "Mary Worth" is not relevant to the examiner; however, the font characteristics in which the name is written can be a critical factor in determining if the travel document is genuine or counterfeit. For this reason, the HSI-FL requires the evidence not be altered or redacted to protect PII. Further, the inclusion of this PII in evidence descriptions and forensic examinations supports law enforcement efforts to detect counterfeit documents and prosecute those who use PII for such purposes. Similarly, for AV materials, the content of the recordings or video is not important to the HSI-FL staff performing the enhancement; however, the content must be unaltered for the enhancement to be successful and useful to the submitter.

Privacy Risk: There is a risk that information provided by submitters to the HSI-FL contains case identifier numbers that link to subjects of investigation. The inclusion of this information in LIMS creates a risk that the HSI-FL is over-collecting PII and putting it at unnecessary risk.

Mitigation: The HSI-FL uses case identifier numbers solely for descriptive purposes to uniquely identify cases in LIMS, allowing for tracking, searching, and retrieving case materials (i.e., evidence, case notes, images, descriptions of evidence, and reports). Submitters provide case identifier numbers and do not include subjects' names. The collection of case identifier numbers that could link to subjects is limited to FBI number, State ID numbers, A-Number, and Incident Number. The inclusion of this information as part of the case information in LIMS is part of the control of evidence that assists law enforcement in verification of chain of custody that supports efforts to prosecute. HSI-FL's security measures and restricted access to evidence, reports, and other case materials reduce the risk of collecting this limited information. The HSI-FL maintains a closed system, with access to LIMS and case materials restricted to those with a need for access and the HSI-FL is subject to regular audits. Evidence received from outside law enforcement agencies is returned only to the submitting agency.

Privacy Risk: During forensic examinations of evidence, there is a risk that finger and palm prints queries against federal databases may return results that incorrectly identify the queried prints as strong matches or "hits" for known prints in the databases. This would increase the likelihood that an individual's prints could be erroneously associated with a criminal investigation or that he or she will be improperly identified as an individual under investigation or suspicion.

Mitigation: The identification of queried prints as strong matches for known prints in specific federal print databases is just an initial step in the print identification process. A trained latent print examiner[11] enters the print query into the Government databases identifying the print only by LIMS case number. Each database will return a list of any existing prints determined to be strong matches based on a print-matching algorithm. The results are identified by their associated number in the database and do not include PII. The examiner compares the characteristics of the print images returned to those of queried prints. If no match is found, the examiner identifies in the case notes as well as the forensic report for the databases queried, that no prints were positively matched, and whether or not the unidentified print has been placed in the unsolved file of the databases.

The name, identification number, and originating database of examiner identified print matches are included in the case forensic report provided to the submitter. This information is also included in the case jacket along with a photograph of the evidence print. The evidence is returned to the submitting agency.

Privacy Risk: Fingerprints of unknown persons that HSI-FL queries in IDENT, ABIS, and NGI (federal print databases) that are not positively matched by HSI-FL examiners may be retained by database owners in unsolved files for indefinite periods of time for the purpose of future print identification.

Mitigation: HSI-FL examiners query prints in federal print databases to support the law enforcement investigations of DHS and other agencies. Information is not shared across federal print databases. Prints are identified only by LIMS case number. No additional information is included with the photographs of prints that are queried.

Prints may be retained by federal print database owners in unsolved files to allow for future identification. Prints must meet certain quality standards set by the system owners to be eligible for retention. Those that meet the standards are retained. When a possible match to that print is identified in the future, the database notifies the HSI-FL, which may reexamine the print queried for determination of a positive match if the case is active or within the case record retention period.

[11] Each latent print examiner completes a valid friction ridge training program, passes a yearly proficiency examination in friction ridge analysis, and is certified or becomes certified within one year of employment or training by the International Association of Identification.

(See section 5.1 for case record retention time periods.) Once a print is positively matched, HSI-FL notifies the database owner(s) so the print can be removed from the database's unsolved files.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The HSI-FL does not provide notice to individuals. Because the information is received directly from other law enforcement agencies or from within ICE, there is no opportunity to provide individuals with direct notification of the collection. When law enforcement agencies collect the information (i.e., documentary evidence, fingerprints) some form of notice may be provided at the time. However, it is unlikely that such notice specifically informs the individual that the information collected will be transmitted to the HSI-FL for forensic examination. ICE and other federal law enforcement agencies engaged in criminal investigations are exempt from providing written notice at the time of information collection pursuant to exemptions for criminal justice agencies under the Privacy Act of 1974 (5 U.S.C. § 552a(j)(2)). Individuals who are the subject of investigations may receive notice during the investigation or prosecutorial stage of their case that evidence or AV materials were submitted to the HSI-FL examinations or enhancements were performed. Release of forensic reports to the defense attorney may also occur. HSI-FL is not involved in these disclosures, as they are the responsibility of the investigating and/or prosecuting agency.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

LIMS does not directly collect information from individuals, and the information received by the HSI-FL for examination is typically collected during the course of a criminal investigation by the submitting agency. Therefore opportunities for the individuals to consent, decline, or opt-out are limited or non-existent.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Because HSI-FL stores information in LIMS that it collects directly from the evidence submitted for examination there is a risk that individuals are unaware of this type of collection, its purpose, how the information is used, and that it is stored in LIMS. Individuals are not provided with notice or the opportunity to consent or decline to have their information collected

and stored in LIMS.

Mitigation: The publication of this PIA and the DHS/ICE-014 Homeland Security Investigations Forensic Laboratory SORN help to mitigate the lack of direct notice to individuals by providing general public notice of the types of records collected and stored by the HSI-FL and the purpose for which these records are created and used. This PIA specifically identifies what HSI-FL records are stored in LIMS. Because this information is used for a law enforcement purposes, direct notification to affected individuals could compromise the existence of ongoing law enforcement activities.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

LIMS case files are unscheduled at this time, and thus are deemed permanent records.

A new schedule is currently being reviewed and once approved will provide retention periods for these records. Once those schedules are approved, the SORN will be updated to reflect the changes. War crimes, terrorism, and homicide cases are proposed to have a permanent record retention schedule. Case information entered into LIMS is proposed to be retained in the system for ten years after the case is closed. The case is "closed" for purposes of retention when the legal proceedings relating to the case have ended.

These retention periods are necessary to allow for the use of case information in support of investigations which continue through the prosecution of crimes. HSI-FL staff may be required to provide testimony in proceedings regarding an offender so retention is necessary to support this need.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information in LIMS will be retained for longer than necessary and appropriate given the purpose of the system and reason for the collection of the information.

Mitigation: Information is retained in LIMS only as long as necessary to complete examinations and support law enforcement investigations and legal proceedings. As these endeavors can span multiple years, retention rates have been set accordingly.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. HSI-FL staff disclose a forensic report of findings (forensic report) to the submitting agency along with the original evidence. Included in the forensic report is the following: the name and address of the requesting agency official, the reference number, and a written explanation of the examiner's findings. If latent print evidence is examined and searched in IDENT, NGI, and/or ABIS, queries and results (positive match information or affirmation that no matches were identified) are included as part of the forensic report. A hardcopy printout of the forensic report and the accompanying evidence is either physically retrieved by the submitter or mailed to the agency official via official courier.

Technical enhancements of AV materials are performed at the request of law enforcement to improve the quality of the materials and clarify details, which allows law enforcement agencies to better examine the materials and develop investigative leads. Materials are returned to the requesting law enforcement agency along with a non-forensic memorandum documenting the enhancements performed. The memorandum and AV materials are retrieved by the submitting agency, mailed to the agency official via official courier, or depending on the AV material being enhanced, may be sent via encrypted email. All information will be used in the conduct of criminal investigations by law enforcement agencies.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of reports and other results of HSI-FL's work with the original submitters of requests supports the identification and arrest of individuals who commit violations of law and to identify potential criminal activity such as the forging of travel and identification documents. This sharing is compatible with the purposes of the original collection, which include the provision of 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 the law; to identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

6.3 Does the project place limitations on re-dissemination?

No, the HSI-FL returns the evidence and provides a forensic report to the original submitter placing no limitations on the re-dissemination of this material. Submitting agencies may need to re-disseminate HSI-FL reports to support the identification and arrest of individuals who commit violations of the law, to uphold or enforce the law in the course of a prosecution, or as required by law for the exoneration or defense of a suspect.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The release of forensic reports are tracked in LIMS along with signed external chain of custody receipts filled out by the seized property specialist and submitters before cases are released. When a forensic examination is completed, an HSI-FL forensic report is generated in LIMS and stored as a read-only PDF File. A hardcopy printout of the forensic report and the accompanying evidence is either physically retrieved by the representative of the submitting agency or mailed via official courier. The report and evidence are tracked by the tracking number generated by the official courier. This tracking number is manually entered into LIMS and used to track the delivery to the submitting agency. The forensic reports are also tracked by tracking numbers and may be provided electronically to the submitting agency through encrypted email attachment upon request. A copy of the signed external chain of custody receipt is loaded into LIMS at the conclusion of each case. These safeguards protect both personal information and the evidence.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that HSI-FL reports containing PII will be shared with or accessed by individuals without a need-to-know.

Mitigation: The HSI-FL shares forensic and non-forensic reports only with the submitter. Transmission methods to return these reports to the submitter are highly secure, including encryption or personal delivery. All transmissions are tracked by chain of custody documentation, which is retained in LIMS. Access to LIMS and the forensic laboratory is highly restricted. The HSI-FL Quality Manual governs control and access to the facility, evidence, and cases. Internal and external audits provide accountability and assist HSI-FL to improve laboratory protections and processes. Reports are created within LIMS itself, which is a closed system within ICE. Access to LIMS is granted only to authorized HSI-FL users for official purposes. LIMS is not accessible to outside agencies or individuals.

Submitting law enforcement agencies have a vested interest in safeguarding information concerning active investigations and limit access and dissemination of information, such as HSI-FL reports, accordingly. Federal agencies are also governed by the Privacy Act, which embodies

fair information practice principles in a statutory framework that restricts sharing of such information and provides criminal and civil penalties for agencies and federal personnel who violate those requirements.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Individuals may request access to records about themselves in LIMS. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests or if the information is compiled in reasonable anticipation of litigation. Providing individual access to records contained in LIMS could inform the subject of an actual or potential investigation, or reveal investigative interest on the part of DHS. Access to the records could also permit the individual who is the subject of a record to impede an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

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 the ICE Freedom of Information Act (FOIA) Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act
500 12th Street SW, Stop 5009
Washington, DC 20536-5009
(202)732-0660

Further information about FOIA/PA requests for ICE records is available at http://www.ice.gov/foia/.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As stated in 7.1, individuals may request access to records about themselves contained in LIMS. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests or if the information is compiled in reasonable anticipation of litigation. Providing individual access to

records contained in LIMS could inform the subject of an actual or potential investigation or reveal investigative interest on the part of DHS. Access to the records could 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. Individuals seeking to amend any incorrect information in LIMS may submit a request in writing as follows:

U.S. Immigration and Customs Enforcement
Privacy & Records Office
500 12th Street SW, Stop 5004
Washington, DC 20536-5004
(202) 732-3300
ICEPrivacy@ice.dhs.gov

Requests must comply with verification of identity requirements set forth in DHS Privacy Act regulations at 6 CFR 5.21(d).

7.3 How does the project notify individuals about the procedures for correcting their information?

Correction procedures are publicized in this PIA and the associated SORN. Because LIMS contains data owned by other agencies, individuals may also have the option to seek access to and correction of their information directly from those agencies that originally collected it.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Because the information in this system originates from other agencies, individuals' rights to be notified of the existence of data about them and to direct how that data may be used are limited.

Mitigation: While LIMS maintains pre-decisional, deliberative information, individuals may still request access to records that DHS maintains about them. Notice on how to file a Privacy Act request about records contained in LIMS is provided by this PIA and the HSI-FL SORN. Individuals can request access to information about them through the Privacy Act and FOIA process, and may also request that their information be amended by contacting the National Records Center. The nature of LIMS and the data it collects, processes, and stores is such that it limits the ability of individuals to access or correct their information. Each request for access or correction is individually evaluated.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

A physical inventory of evidence sent to the laboratory for analysis is conducted twice a year by the LIMS Program Manager and an assigned employee. The evidence is maintained and inventoried by a trained evidence custodian. The physical records are compared with the data entered into LIMS during audits that are conducted twice a year. The requirements for conducting inventories and physical checks as well as guidance concerning the handling of requests, evidence, and other preventative measures are outlined in the Homeland Security Investigations Forensic Laboratory Quality Manual. In addition, the ISSO performs weekly reviews of the system audit logs to ensure that no evidence records were altered during the period of review. Any error is reported to the LIMS Program Manager and the HSI-FL Laboratory Director for investigation.

The work product entered into LIMS is continuously reviewed by HSI-FL supervisors. The audit logs of the physical evidence should reflect the same information that is captured within LIMS. The audit log captures the following information: ad-hoc query tools, agency search, barcode search, country search, county search, when a user prints a report from within LIMS, evidence search, fire arms search, lab case number search, when a user accesses the main case view of any case, name search, offense search, other identification search, and when a user views or edits results. The supervisor and the system administrator can review the audit logs at any given time.

LIMS restricts view and modify permissions for individual case information to those with a “need to know” basis. This means that standard users will only have the ability to modify cases that are assigned to them. For cases that are not assigned to them, standard users will only be able to view the case information. They will not have permission to modify that information. If a standard user wishes to modify a case not assigned to him or her, he or she must obtain approval from management. The manager must request that the system administrator change the user’s permissions for that case. All modifications to user permissions are logged into an automatic audit log. Four designated individuals, including the supervisor, two LIMS program managers, and the database administrator, have access to full audit trails in LIMS. System administrators cannot, however, modify or delete the audit log.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All ICE employees and contractors complete annual mandatory privacy and security training, specifically the Culture of Privacy Awareness Training and the Information Assurance Awareness Training. All HSI-FL staff members are expected to demonstrate and promote high standards of professionalism and are responsible for appropriately safeguarding their work areas and personal workspaces including evidence and information obtained in their official capacities in accordance with the Homeland Security Investigations Forensic Laboratory Quality Manual.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Direct access to LIMS is limited to authorized HSI-FL personnel conducting official analysis activities. User access to LIMS is controlled by HSI-FL supervisors in cooperation with the LIMS System Administrator. A user's data access rights are determined by the level of permissions granted in accordance with the user's system profile. The System Administrator provides access for HSI-FL staff only after receiving approval from the Laboratory Director or designated representative.

Approval is granted after the staff member's first line supervisor submits a completed IT Account Access form to the System Administrator, copying the Laboratory Director or Representative, requesting an account for the staff member specifying the type of user roles/levels of permission the employee is to be assigned. The Laboratory Director or Representative reviews the request and then sends approval the System Administrator who creates the account, assigns a user ID, and temporary password to provide access to LIMS.

Users' access and usage rights are restricted in the LIMS system based on job duties and responsibilities. Each user's access is restricted to a "need to know basis" to perform particular duties. The following user roles are assigned within LIMS:

- General Users: General Users are categorized based on their specific job responsibilities in the following sections: Questioned Document, Forensic Fingerprint, Operations, and Seized Property Specialist. Staff members in each section have designated duties and roles assigned to them in LIMS. Each user can view all case related data in LIMS but only persons assigned to a case can edit or modify that case. General users cannot delete a case.
- Supervisors: Supervisors require special access that is authorized by the Laboratory Director. Supervisors' rights in LIMS are limited to the functions and capabilities to support a supervisory role. This includes assigning cases to specific users, reviewing and closing cases, and editing all cases assigned within their section.

- Information Special Security Officer (ISSO): The ISSO's capabilities are limited to reviewing audit logs and producing recurring reports for ISSO reporting.
- Data Base Administrator (DBA): The DBA requires special access rights that are limited to the unique system capabilities required to perform database modifications, updates, or changes.
- System Administrator (SA): The SA has full control over the system. The SA can perform user role changes, system configurations, changes or updates, and general administrative work for the system. The SA role is limited to users specially selected by the Laboratory Director.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any new uses or sharing of LIMS information would be vetted through the ICE and DHS Privacy Offices prior to implementation. This would ensure that any such uses were compatible with the original purposes for which the data was collected, and that this PIA and the DHS/ICE-014 SORN were updated, if required. ICE does not expect to enter into data sharing agreements or MOUs with respect to the information maintained in LIMS, or to grant user access to individuals outside of ICE.

Responsible Officials

Amber Smith
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security