Privacy Impact Assessment

for the

Laboratory Information Management System

DHS Reference No. DHS/ICE/PIA-046(a)

February 1, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Office of Homeland Security Investigations (HSI) owns and operates the Laboratory Information Management System (LIMS) as part of its Forensic Laboratory. The HSI Forensic Laboratory (HSI-FL) implemented LIMS to facilitate and store data related to the scientific authentication, examination, research, and analysis of documents and the enhancement of audio-visual (AV) materials. HSI-FL also examines latent finger and palm prints found in the field. This Privacy Impact Assessment (PIA) update is being published to provide transparency regarding a new subsystem within LIMS called LatentCD, which allows the HSI-FL Latent Print Unit to ingest and manage the workflow of unidentified latent prints.

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.

HSI-FL Latent Print Unit

One of the examination sections at HSI-FL is the Latent Print Unit, which provides finger and palm print services to support law enforcement investigations. A latent print is an impression of the friction ridge skin of the fingers, palms, or soles of the feet that has been transferred to another surface.[1] Law enforcement organizations collect latent prints in investigations as evidence because of their identifying features. Latent prints can be compared to the stored fingerprints of known or unknown suspects in an investigation to assist in identifying the owner of the prints. The HSI-FL Latent Print Unit's examiners process and examine latent prints, compare latent and inked prints, and conduct automated fingerprint searches through a variety of federal databases. Latent print examiners process latent finger and palm prints on all types of evidence to include firearms, drug packaging, currency, periodicals, photo albums, CDs, and computers. HSI-FL will provide results from these examinations to investigators which may then be used in law enforcement investigations and/or admitted into evidence in judicial proceedings.

LIMS

As a crime laboratory, the HSI-FL is accredited in the forensic science disciplines of

[1] *See* ISO/IEC 19794-4:2005, Information technology — Biometric data interchange formats — Part 4: Finger image data *available at* https://www.iso.org/obp/ui#iso:std:iso-iec:19794:-4:ed-1:v2:en.

forensic document and friction ridge examination by the American National Standards Institute (ANSI) National Accreditation Board (ANAB) consistent with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) joint standard ISO/IEC17025.[2] 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 accreditation requirements. LIMS is a commercial off-the-shelf product customized to meet HSI-FL requirements and can only be accessed by HSI-FL personnel.[3] 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 generates reports of HSI-FL activities and findings. It also captures other case-related activities such as descriptions of expert witness testimony provided by HSI-FL examiners.

LIMS stores requests by state, local, and federal law enforcement agencies (HSI-FL customers) for status updates on forensic examinations and general case-related inquiries. 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 documents and/or print examinations.

HSI-FL 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 a forensic examination of evidence.[4] Investigators may ship, physically deliver, or send requests electronically via encrypted email to the HSI-FL.[5] For example, investigators may submit travel and identity documents to the HSI-FL to determine authenticity and the presence of alterations. The Latent Print Unit performs detailed and complex examinations of latent and inked impressions from evidence to the known or unknown impressions of subjects. The unit also searches for matching prints within the DHS Office of Biometric Identity Management's (OBIM's) Automated Biometric Identification System (IDENT)[6]—to be replaced by the

[2] *See* ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories, *available at* https://www.iso.org/standard/66912.html.
[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE LABORATORY INFORMATION MANAGEMENT SYSTEM (LIMS), DHS/ICE/PIA-046 (2016), *available at* https://www.dhs.gov/privacy-documents-ice.
[4] ICE field offices ensure an ICE statutory nexus when requests are made by state, local, and federal law enforcement agencies. These agencies do not have direct access to use the lab or submit without ICE's approval to do so.
[5] Submitters complete ICE Form 73-0003, *Request for Laboratory Examination*, documenting submitter information, case information, and types of examinations requested.
[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE DHS AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Homeland Advanced Recognition Technology System (HART)[7]—the Federal Bureau of Investigation's Next Generation Identification (NGI) System,[8] and the Department of Defense's Automated Biometric Identification System (ABIS).[9]

Upon receiving a request, an HSI-FL seized-property specialist reviews the evidence, creates a case in LIMS, and 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. LIMS captures all access and use data for each case, which supports auditing and accountability and chain of custody requirements, as well as the privacy, security, quality, and integrity of personally identifiable information (PII) in LIMS.

Once LIMS generates the case record number, the seized property specialist assigns the case to a HSI-FL examiner and stores the evidence in the HSI-FL secure evidence room. LIMS notifies the HSI-FL examiner of the case assignment when they access LIMS. 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, this description may contain real or fictitious PII (e.g., names, passport numbers). HSI-FL has the capacity to conduct searches using 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.[10]

---

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[8] *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, and Fingerprint Identification Records System SORN, *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-01-25/pdf/E7-1176.pdf.

[9] *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.

[10] HSI-FL is not given any information regarding the details of the case (e.g., crime committed) upon submission. Submitters only provide respective case identifying numbers, although travel and identity documents, for example, may include additional PII such as name, address, or date of birth.

When an examiner takes custody of evidence for latent print examination, they will develop latent prints using processes that render the prints visible. The examiner photographs visible or developed latent prints, saves them to a CD that is retained in the case jacket and stored with the physical file, and uploads the digital images to LIMS. The examiner conducts the examination of the prints 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 may also be queried in the NGI system. The examiner manually enters queries and any positive matches to the prints' owner into LIMS in the form of examination materials and case notes.

When examiners query a database to identify a latent print, they only include the LIMS case number with the print. Each database will return a list of any existing known 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 other PII. The examiner compares the characteristics of the print images returned to those of queried prints. If no match is found, the examiner records the results in the case notes and provides a forensic report outlining the databases that were queried, indicating that no prints were positively identified, and stating whether or not the unidentified print had been placed in the unsolved fingerprint file of the databases. When a latent print examiner determines there is a potential positive identification in another 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, noncitizen A-number (if available), and images of finger/palm prints.

After the examiner concludes their exam, the HSI-FL staff provides 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 (provided by the agent during original submission), LIMS case number, and a written explanation of the examiner's findings. 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.

Reason for the PIA Update

HSI-FL is adding a subsystem to LIMS to help manage the workflow of the HSI-FL Latent Print Unit called LatentCD. LatentCD will modernize HSI-FL's existing manual process. Before LatentCD, examiners documented details of the evidence they examined and steps they took during the examination process using fillable PDFs that allowed open-text fields for examiner case

notes. Examiners could print and physically mark-up[11] images of the latent prints or upload the images to a secondary software which allowed examiners to digitally mark up the latent print. At the conclusion of the exam process, the examiner would print case note PDFs (as prepared by the examiner) and include the PDF in the case documentation. Printed photos were kept with the case documentation. Examiners would also upload marked up digital photos to LIMS.

LatentCD allows latent prints to be uploaded directly into LIMS and negates the need for secondary software to digitally mark the print. LatentCD provides the necessary tools to convert the HSI-FL latent print examination process into a systematic electronic workflow. The software provides a group of specialized tools and features specifically for latent identification documentation and comparative analysis. These tools include simple side-by-side onscreen comparison of prints, documentation and charting of key latent characteristics, and the ability to enter and track case notes within LatentCD. This software automates the natural steps in a latent print workflow process, standardizes documentation practices among examiners, and provides overall consistency throughout the unit.

Privacy Impact Analysis

Authorities and Other Requirements

The inclusion of LatentCD to LIMS has not changed the authorities for HSI-FL's collection of data, nor its retention schedules for data which resides within LIMS. Pursuant to the Homeland Security Act of 2002 (Pub. L. No. 107-296, Nov. 25, 2002),[12] 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 the U.S. Code. The Secretary delegated this authority to ICE.[13] HSI-FL has collected latent prints throughout its existence as a forensic lab. LatentCD has only streamlined and digitized the standard workflow of the HSI-FL Latent Print Unit.

Characterization of the Information

LatentCD does not change the types of information collected by HSI-FL, but it does allow HSI-FL to ingest latent prints into LIMS. When the LIMS PIA[14] was first published, and prior to LatentCD, an examiner would photograph and develop latent prints, upload the digital file to

[11] Relating to latent fingerprints, the term "mark-up" defines when an examiner uses colors and symbols to note findings. Markups are useful when presenting fingerprint evidence and findings to attorneys, judges, and jury members. Marking up does not involve altering the fingerprints in any way.
[12] 6 U.S.C. § 142(a)(2).
[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, 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) *available at* https://www.hsdl.org/?view&did=234774.
[14] *Supra* note 3.

LIMS, and save them to a CD that was retained in the case jacket and stored with the physical file. Examiners would utilize secondary software to mark findings made by the examiner during their examination process. Those markups were then printed and stored in the case jacket and digitally uploaded in LIMS. In 2019, the American National Standards Institute National Accreditation Board, in light of ISO/IEC 17025, mandated that federal agencies document the analysis and comparison phases in examining prints. To comply with this requirement, HSI-FL acquired software that allows such documentation. With LatentCD, the HSI-FL examiners do not require the use of secondary software to note their findings. LatentCD converts a paper-based process into a digital workflow contained in LIMS. Both the latent prints and the case notes made by the examiner are contained in LIMS as well as the case jacket.

Privacy Risk: There is an increased risk that duplicating latent prints in LIMS increases the chance of compromising the information.

Mitigation: This risk is mitigated. LatentCD is a safer option in retaining information than previous processes and reduces the need to create duplicates of data. Paper copies of examination materials can be lost or misplaced. Secondary software requires transfer of information to multiple locations before the information can be uploaded into LIMS. The LatentCD software allows the examiner the opportunity to create all documentation and case notes in LIMS with no additional steps or transfers. The LatentCD software allows the examiner to directly input all case examination information. Secondary software is time consuming and creates a greater possibility of errors occurring during data transfer. The LatentCD software ensures that all activities the examiner is working on will cross into LIMS as the two systems are directly connected. LatentCD creates an entirely electronic process and omits the need for paper copy retention.

Privacy Risk: There is a risk that latent fingerprints collected at crime scenes from individuals who are not perpetrators may be retained inappropriately in LIMS.

Mitigation: This risk is partially mitigated. HSI-FL retains all latent prints it collects per the Federal Rules of Evidence[15] and American National Standards Institute National Accreditation Board requirements for forensic laboratories. Any friction ridges that are observed or developed in a case and are of value for comparison purposes must be retained per accreditation standards. This includes observed or developed prints that may have been determined by a submitter to have no bearing on the case (e.g., exclusionary prints or prints from someone with no knowledge of the crime). Within LIMS, prints that have not been matched to an owner are referenced only by case number and exhibit number. No PII is attached to latent prints unless the prints are positively matched to an individual.

LatentCD is not a resource for saving data, but rather is a program that aides in electronically transferring all case notes and images into LIMS. The LatentCD software limits the

[15] Federal Rules of Evidence, Pub. L. No. 110–322, § 901(a), 122 Stat. 3537 (2011).

amount of information attached to any particular image and does not require additional information for a print's retention in LIMS. Moreover, neither LIMS nor LatentCD are biometric databases like IDENT, NGI, or ABIS. Examiners must initiate biometric searches of prints outside of LatentCD and LIMS to determine if the prints match to an identity within those databases. Thus, while LatentCD may retain prints unrelated to a target of an investigation, those prints are only accessible to HSI-FL latent print examiners, are retrievable only by LIMS case number, and are not searchable via biometric modalities in LIMS.

Uses of the Information

LatentCD is a subsystem that allows for the ingestion of latent prints into LIMS and digitizes the workflow of the HSI-FL Latent Print Unit. LatentCD does not algorithmically analyze, match, or identify latent prints; it is merely a case processing and workflow management tool. The entire examination process of a latent print is conducted by HSI-FL personnel; however, the examination process will now be digitally documented in LatentCD rather than using manual paper-based processes and secondary software. All information related to HSI-FL's examination will be stored in LIMS. The evidence packaging, evidence description, processing performed, and results from biometric searches will be input into LatentCD, which will then use the information to automatically fill case notes. When latent prints are present, digital images of latent prints will be imported into LatentCD to allow examiners to digitally document their processes and findings.

Within LatentCD, original latent images cannot be altered. If an examiner enhances or makes a markup of the latent print, those edits are saved automatically as overlay versions of the original image. The software maintains digital image integrity, maintaining a full image history and reporting module for all digital enhancements and chain of custody. The original image is always maintained and never altered.

LatentCD functionalities include:

- Single or batch image upload and image export;
- Visual directory and definable database searches within LatentCD to find cases;
- Metadata display viewer and report, which documents all enhancements and modifications made by an examiner during analysis;
- Image history viewer, which allows examiners to see previous overlays on an image and access them at any time;
- Basic annotation and markup tools;
- Basic image enhancement tools (Brightness/Contrast) and image filtering tools (e.g., levels, invert, auto level) to clarify a print, reduce distortion, and reduce background interference in an image;
- Overlay grouping tools that group enhancements made by an examiner so work does not affect the original image and different iterations of work can be isolated or accessed;

- Latent print orientation tools and image rotation/movement tools;
- Multi-Image Workspace Display, which allows examiners a side-by-side comparison of prints;
- Image charting tools with image positioning/anchoring that allows for examiners to highlight key characteristics on an image; and
- Measurement Tools.

At the conclusion of the exam, case note printouts are prepared by LatentCD (based on examiner inputs) as digital files to be included in the case documentation. These printouts will be consolidated by HSI-FL to create a forensic report that will be returned to the agency that submitted the latent print for examination.

Privacy Risk: There is a risk that incorporating LatentCD into LIMS will allow unauthorized users access to latent prints and related case notes.

Mitigation: This risk is mitigated. LatentCD software is only accessible by the HSI-FL Latent Print Unit staff. No other forensic units or personnel have access to sign in, alter, change, or delete any of the information within LatentCD. LatentCD shares many of the same user access restrictions as LIMS to ensure that only individuals with a need-to-know have access to the data. HSI-FL has also limited the number of authorized users of the LatentCD software to only those members of the Latent Print Unit, precluding other individuals from creating new accounts. Moreover, while the LatentCD software is integrated with LIMS, LatentCD only physically resides on workstations and laptops that are assigned to the Latent Print Unit. Personnel from HSI-FL that work in different units at the laboratory therefore cannot physically access LatentCD.

Privacy Risk: There is a risk that the latent prints may be digitally altered or compromised within LIMS and then used improperly.

Mitigation: This risk is mitigated. The LatentCD software is a tool utilized by the HSI-FL Latent Print Unit examiners to enhance images, document analysis and comparison phases, and digitally write case notes. All images are obtained through a digital capture photography system technology located within the Latent Print Unit. As with all other access, only latent print examiners have access rights to the photography system. The unprocessed read and write (RAW) image is retained in the case file automatically. The software does not have the ability to alter or change the RAW images. All examinations are conducted on copies of the RAW file and are saved, along with all digital audit trails, within the LatentCD software.

In addition, LIMS restricts access permissions for individual case information to those with a need-to-know. All user permissions are logged into an automatic audit log. The system Information Special Security Officer (ISSO) performs weekly reviews of those audit logs and reports any errors or improper use to the LIMS Program Manager for further inquiry.

Notice

LatentCD does not materially alter the privacy risks of LIMS or HSI-FL operations regarding notice to individuals. HSI-FL does not collect information directly from individuals, and, due to the law enforcement nature of its work, cannot give notice to individuals when it acquires their information. Notifying individuals that their information is associated with a criminal investigation may give suspects opportunity to hamper or impede the law enforcement investigations HSI-FL supports.

Privacy Risk: There is a risk that individuals will be unaware that their latent prints are being retained in LIMS.

Mitigation: This risk is partially mitigated. The original LIMS PIA and this PIA update provide general notice that LIMS stores latent prints. Moreover, HSI-FL has collected and retained latent prints since its inception as a forensic lab. Individuals who are the subject of investigations may also receive notice during the investigation or prosecutorial stage of their case that evidence was submitted to HSI-FL. HSI-FL is not involved in these disclosures, as disclosing this information is the responsibility of the investigating and/or prosecuting agency.

Data Retention by the Project

LIMS case files are unscheduled at this time, and thus are deemed permanent records. This includes latent prints uploaded into the system. HSI-FL is creating a records retention schedule in consultation with the ICE Records and Data Management Unit. ICE has proposed that war crimes, terrorism, and homicide cases have a permanent record retention schedule. This retention schedule will be consistent without regard to the original submitter's affiliation (state, local, federal law enforcement agency). ICE also proposes that other case information entered into LIMS 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.

Privacy Risk: There is a risk that latent prints may be maintained in LIMS beyond what is necessary and appropriate for their collection.

Mitigation: This risk is not currently mitigated. Until a records schedule is completed and approved by the National Archives and Records Administration (NARA), HSI-FL is required to retain all records as permanent. When the schedule is approved, however, HSI-FL has staff dedicated to records maintenance and quality assurance. That staff will review all case files and associated documents to determine the appropriate date of destruction. If a record is found to be past its required retention date, the staff will manually purge the records from LIMS and LatentCD. This requirement is not unique to LatentCD, and will be implemented throughout HSI-FL.

Information Sharing

There is no change to the information sharing privacy risks of LIMS or HSI-FL through its use of LatentCD. HSI-FL may share information with biometric databases (such as IDENT/HART, NGI, or ABIS) to run queries against their systems. HSI-FL will also share case notes, results, and reports regarding a case with the submitting HSI-FL customer. All information sharing conducted by HSI-FL is conducted outside of LatentCD and continues to be in accordance with the previously published LIMS PIA.[16]

Redress

The access, amendment, and redress procedures continue to be the same for LIMS and HSI-FL. Individuals may request access to records about themselves in LIMS and LatentCD. 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 ICE or the HSI-FL customer. 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 Office
500 12th Street SW, Stop 5009
Washington, DC 20536-5009
(202) 732-0660

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

[16] *Supra* note 3.

Auditing and Accountability

LatentCD does not change the auditing and accountability practices of LIMS or HSI-FL as outlined in the previously published PIA. LIMS and HSI-FL are subject to rigorous auditing and accountability requirements to maintain accreditation as a forensic laboratory. As a subsystem of LIMS, LatentCD is subject to the same requirements.

Contact Official

Mindi S. Ramage
Unit Chief
Homeland Security Investigations Forensic Laboratory
U.S. Immigration and Customs Enforcement
(703) 285-8731
(202) 903-5401
Mindi.S.Ramage@ice.dhs.gov

Responsible Official

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717