Privacy Impact Assessment Update
for the

Laboratory Evidence and Information Management System (LEIMS)

DHS/USSS/PIA-018(a)

August 21, 2019

Contact Point
Edna G. Rucker
Privacy Officer
United States Secret Service
(202) 406-5357

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

Abstract

The United States Secret Service (USSS or Secret Service) has a Laboratory Evidence and Information Management System (LEIMS) that is used to support agency forensic and laboratory personnel. The LEIMS generates and manages a variety of operational and sample processing data, while meeting stringent requirements for traceability, chain of custody, evidence handling, and compliance with legal and regulatory statutes. The Privacy Impact Assessment (PIA) update is being conducted to document that LEIMS no longer supports the USSS Forensic Services Division (FSD). Only the USSS Special Services Division (SSD) remains supported by LEIMS.

Overview

The LEIMS is a commercial off-the-shelf (COTS) product that supports Secret Service SSD's laboratory information management needs. The LEIMS application continues to provide a user-friendly means for the collection and analysis of a wide range of information generated from SSD laboratory workflows.

LEIMS will continue to house general information from USSS employees and contractors working on behalf of USSS (i.e., LEIMS users) and information from individuals and agencies that receive services from SSD (i.e., customers and partners). This general information includes names, business e-mail addresses, and business phone numbers for the purposes of developing contact lists for notifications (e.g., notification that a process, such as sample analysis, is complete). In addition, LEIMS users must log into LEIMS so that LEIMS can document activities and modifications made by users for quality control purposes. Defined user classes will restrict user access so that users are using LEIMS only as needed for their official job duties.

LEIMS may also collect and retain any information that is included with items that are sent to SSD facilities for screening or analysis. PII collected from these items generally includes the names, addresses, and phone numbers of senders and recipients. This information is routinely collected when real or potential threats are identified during the screening process. Documentation of processed items can also include written descriptions and photographs, and is routinely shared within USSS following standardized procedures and on an as-needed basis when information is required by investigative leads (e.g., cases involving real or potential threats). Information is not routinely shared within DHS components or with external partners, but may be shared with law enforcement partners who have a need-to-know, due to an open investigation.

Reason for the PIA Update

The reason for this update is to reflect that LEIMS no longer supports FSD. Capabilities such as tracking evidence items, case information, chain of custody transactions, analytical notes, results, and examiner reporting for Forensic Service Division no longer exist within LEIMS system. These functionalities are now conducted internally within the Forensic Service Division System.[1]

Privacy Impact Analysis

Authorities and Other Requirements

LEIMS is covered by the DHS/USSS-001 Criminal Investigation Information System of Records Notice (SORN).[2] LEIMS has a completed documented system security plan per the ATO that was granted on December 3, 2018.

LEIMS issues data and reports associated with evidence for law enforcement and protective services that can be discarded only in accordance with the applicable disposition schedule associated with the systems within which they are maintained. To the extent that LEIMS data and report information are incorporated into an agency system of records, such information would be covered by the retention schedule applicable to that record type. For example, criminal investigative records are covered in the DHS/USSS-001 Criminal Investigation Information SORN, and would be subject to the retention schedules outlined within that SORN.

The information that will be entered into the LEIMS is not covered by the Paperwork Reduction Act.

Characterization of the Information

There are three categories of individuals on whom information is likely to be collected in LEIMS: A) LEIMS users; B) external government users of facility services (i.e., federal customers and partners); and C) individuals whose information is included with items that were submitted to SSD for protective or investigative analysis.

LEIMS users include USSS employees and contractors working on behalf of USSS. Examples of potential PII collected for this category include names, business mailing addresses, business telephone numbers, business e-mail addresses, business zip codes, business facsimile numbers, qualification records, and certificates (e.g., facility-specific training required prior to performance of duties). Individuals will directly provide this information.

---

[1] For more information *see* DHS/USSS/PIA-017 Forensic Services Division System (FSDS), *available at* https://www.dhs.gov/publication/dhsussspia-017-forensic-services-division-system.
[2] DHS/USSS-001 Criminal Investigation Information System of Records, 76 FR 49497 (August 10, 2011).

The only PII collected external government users of facility services is business contact information. Examples of potential PII collected from these client organization representatives (i.e., federal customers and partners) include names, business mailing addresses, business telephone numbers, business e-mail addresses, business zip codes, and business facsimile numbers. Individuals or their representatives will directly provide this information.

There is the potential that information collected, in text or photograph format, during the screening of items could include PII (e.g., sender and recipient information). This information is routinely collected for investigative use in response to an actual or potential criminal threat. LEIMS will be capable of preparing reports that may include text and photographic descriptions of items associated with potential threats or criminal acts. This information is routinely shared only with USSS personnel with a need-to-know, in order to support the agency's protective and investigative missions.

Information taken from screened items belonging to members of the public that is submitted by law enforcement sources will be entered into LEIMS by USSS employees or contractors working on behalf of USSS.

For items including PII that are submitted to SSD for protective or investigative analysis, it is the responsibility of the submitter to verify PII accuracy. In the event that a recipient of LEIMS reports becomes aware of any inaccuracies in PII, SSD will take corrective actions for any PII that is input incorrectly.

Uses of the Information

LEIMS collects only the PII required for managing evidentiary material and/or developing investigative leads in accordance with USSS mission functions and authorities. With regard to SSD LEIMS users, customers, and partners, PII is collected in order to verify access and authority to request and receive services provided by SSD. Additionally, PII is collected from USSS employees and contractors working on behalf of the USSS to manage access and as required to associate evidence and item processing with the individuals involved with processing it.

LEIMS also uses PII to prepare lists of LEIMS users and send notifications to LEIMS users as necessary (e.g., identifying individuals that need to complete a facility required training and sending a notice to those individuals that are past due for completion of the training). Notifications are also routinely sent to external government users of facility services.

There are no other components with assigned roles and responsibilities related to LEIMS. Other components may receive information managed in LEIMS (e.g., summary test reports), but they do not have direct access to the data. That information is provided only after an authorized USSS LEIMS user has verified the requester's authorization and need-to-know the information.

Notice

There are no changes in notification procedures with this update.

Data Retention by the project

There are no changes in data retention with this update.

Information Sharing

There are no changes in external sharing and disclosure with this update.

Redress

Access, redress, and correction have not changed with this update.

Auditing and Accountability

All FSD users' access to LEIMS has been removed. The system will continue to take all necessary measures to ensure that the information stored within is used in accordance with the stated practices in the underlying PIA. All USSS information systems are audited regularly to ensure appropriate use of and access to information. Specifically related to this system, application access is mediated through a two-tier identification and authentication process. Any changes to the hardware or software configuration are subject to review and approval by the USSS Configuration Control Board process to ensure integrity of the application.

Responsible Official

Edna G. Rucker
Privacy Officer
U.S. Secret Service

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

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