Privacy Impact Assessment
for the

Laboratory Evidence and Information Management System (LEIMS)

DHS/USSS/PIA-018

May 23, 2017

Contact Point
Latita M. Payne
Privacy Officer
United States Secret Service
(202) 406-5838

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) is creating the Laboratory Evidence and Information Management System (LEIMS) to support agency forensic and laboratory personnel. The LEIMS will generate and manage 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. While the primary objectives of this system do not include the collection of personally identifiable information (PII), USSS is conducting this Privacy Impact Assessment (PIA) because some descriptive records in LEIMS may include PII. The system may also track the names and contact information for Special Services Division (SSD) and Forensic Services Division (FSD) customers, and the activities of LEIMS users.

Overview

The United States Secret Service (USSS or Secret Service), Special Services Division (SSD) and Forensic Services Division (FSD) are procuring a Laboratory Information Management System (LIMS), a commercial off-the-shelf product, as a baseline to create the Laboratory Evidence and Information Management System (LEIMS). The LEIMS application will provide a user-friendly means for the collection and analysis of a wide range of information generated from SSD and FSD laboratory workflows. The LEIMS database will store logistical, administrative, and incident-specific data. Examples of data collected by LEIMS include item handling time, sample handling time, sample analysis, operational incident details, laboratory and analytical equipment maintenance, laboratory consumable usage and inventory, chain of custody for items and samples, and personnel training.

LEIMS will also 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 and FSD (*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 and FSD 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.

The LEIMS request for proposal included a requirement that the vendor solution be compliant with 48 CFR 52.239-1: Privacy or Security Safeguards.[1] All LEIMS deliverables shall comply with the applicable technical and functional performance criteria of this PIA and applicable Systems of Record Notices (SORN). Information retained in LEIMS will be covered by the DHS/USSS-001 Criminal Investigation Information System of Records.[2]

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?

The collection of information is authorized by the Secret Service's protective authority contained in 18 U.S.C. § 3056 A - Powers, Authorities, and Duties of United States Secret Service.

Data is retained only as authorized under 50 U.S.C. § 501a3, E.O. 12333, and DHS Management Directive 10052. Investigative information is solicited and obtained under the authority of the Federal Records Act.[3] Information is collected from criminal investigations, such as threats to protectees, terrorism, financial, counterfeit, cyber-crimes, kidnapping, child pornography, homicide, and identity theft. Such investigations are authorized by 18 U.S.C. §§ 3056 - Powers, Authorities, and Duties of United States Secret Service, 1029 - Fraud and Related Activity in Connection with Access Devices, and 1030 - Fraud and Related Activity in Connection with Computers.

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

LEIMS is covered by the DHS/USSS-001 Criminal Investigation Information System of Records.

---

[1] 5 U.S.C. § 552a, "Records maintained on individuals."
[2] *See* DHS/USSS-001 Criminal Investigation Information SORN, 76 FR 49497 (August 10, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.
[3] 44 U.S.C. § 3101, "Federal Records Act" (Title 36, Code of Federal Regulations, chapter XII).

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

Yes. A draft system security plan has been completed for the LEIMS. Development of a Certification and Accreditation Package and a security plan are contractor requirements included in the performance work statement. Authority to Operate is expected to be granted by September 28, 2017.

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

LEIMS issues data and reports associated with evidence for law enforcement and protective services and 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 those SORNs.

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.

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

Section 2.0 Characterization of the Information

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

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 or FSD for protective or investigative analysis.

LEIMS users will include USSS employees and contractors working on behalf of USSS. Examples of potential PII collected for this category includes 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). LEIMS is expected to be capable of preparing lists of LEIMS users and sending 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. The only PII collected on these individuals is business contact information. Examples of potential PII collected from 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.

Forensic Services case information can also include dates of birth, Social Security numbers (SSN), assigned Federal Bureau of Investigation (FBI) numbers, and agency arrest information/booking numbers. LEIMS is expected to be capable of sending routine e-mail notifications to internal and external users of USSS screening and forensic services.

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.

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

Individuals or their respective organizations will directly provide business contact information, qualification records, certificates for USSS employees and contractors working on behalf of USSS, and business contact information for external government users of facility services.

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.

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.

For items including PII that are submitted to SSD and FSD 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 or FSD will take corrective actions as appropriate. Inaccurate information included in documentation submitted by external sources, but stored in the LEIMS, would not typically be corrected unless the inaccuracy was due to an administrative data entry error at SSD or FSD.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that LEIMS could collect information about individuals who pose no threat, particularly information received by SSD or FSD from concerned citizens regarding a potential threat that may require protective or investigative analysis.

Mitigation: This risk is partially mitigated. Trained and experienced agency personnel direct the handling of evidentiary and investigative materials and only information that is deemed necessary for the furtherance of the agency's missions is entered into LEIMS. For example, a Special Agent evaluates an item that may include a criminal threat. If the trained and experienced Agent determines that no threat exists, no item detailing unrelated information would be collected and entered into LEIMS.

Privacy Risk: There is a risk that LEIMS could collect more PII than is necessary to accomplish its mission.

Mitigation: This risk is partially mitigated. The Secret Service collects the information necessary to enable positive identification so that: (a) the individual is identifiable during future interactions with the agency; (b) the individual is not erroneously identified as, or erroneously linked to, another individual; and (c) further investigation can be conducted, if necessary. In addition, information gathered from items submitted for analysis that contains PII data (*e.g.*, items in text or photograph format that contain PII) is processed as evidence or potential investigative material. The LEIMS is not designed for storage of PII from items that do not specifically relate to the agency's investigative and protective missions.

Privacy Risk: There is a risk that LEIMS will collect and report incorrect PII that may be used in an investigation.

Mitigation: LEIMS uses PII present on evidentiary or investigative material solely for descriptive purposes, to uniquely identify evidence submitted for examination. No assessment is made of an individual whose PII is present on examined evidence or whose information may be linked to a case identifier. For example, a photograph of a crime scene may include an individual's address in the picture, but that data is not captured as PII separate from the photo or the item's text

description and submitter information. It is simply handled as photographic material and treated as law enforcement or investigative evidence. Sender information and text fields are searchable and can be set up to alert LEIMS users if listed keywords or names are entered into the system.

In the event of an investigation, Secret Service personnel who have received specialized training in investigative and analytical techniques review all pertinent information and conduct research to verify the information, including the accuracy of the collected PII if received as part of the evidence/items being processed.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses 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. PII is collected to track evidence/items through the handling/examination process to ensure its integrity. With regard to SSD and FSD LEIMS users, customers, and partners, PII is collected in order to verify access and authority to request and receive services provided by SSD and FSD. 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.

Any PII included with the evidence is protected as evidentiary material and released only as part of that evidence to verified individuals authorized to receive it.

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. 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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII collected by LEIMS may be used by USSS personnel for an improper and/or unauthorized purpose.

Mitigation: Access to LEIMS is limited to a specific number of agency users and is controlled by the system's secure IT infrastructure, which requires login, logs activity, and uses firewalls, as well as other computer security measures. To ensure the information is used consistently with the purposes of the original collection, USSS employees with an official need-to-know are trained in the proper use and handling of information identified by LEIMS as well as PII.

Section 4.0 Notice

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

In addition to this PIA, the DHS/USSS-001 Criminal Investigation Information SORN provides notice regarding the collection of information and the routine uses associated with LEIMS. Advanced notice of the collection of information to investigative targets or others involved in an investigation generally is not provided as it would compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings. The final rule for the Criminal Investigation Information System SORN exempts the system from portions of the Privacy Act.[4]

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

The collection of information in LEIMS is to investigate evidence or items involved in the investigation. Thus there are no opportunities for individuals to consent to, decline, or opt out of the project because doing so could compromise ongoing law enforcement investigations and otherwise impede law enforcement proceedings.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of LEIMS and the data it collects and maintains.

[4] *See* Implementation of Exemptions; DHS/USSS-004 Protection Information Systems, 74 FR 45090 (August 31, 2009), *available at* https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/pdf/E9-20755.pdf.

Mitigation: Due to the nature of the information maintained in LEIMS, this risk cannot be fully mitigated. This PIA and the DHS/USSS-001 Criminal Investigation Information SORN serve as public notice of the existence of LEIMS, the data it collects and maintains, and the routine uses associated with the information collected.

Section 5.0 Data Retention by the project

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

Information that is collected that becomes part of an investigative case file will be retained for a period that corresponds to the specific case type developed. The retention periods established and/or approved by NARA for investigative case files may cover periods as short as two years, or indefinitely (such as for threats to the President and homicide cases), depending on the type or disposition of the case.

Per USSS Records Disposition Schedule N1-87-10-4 (approved by NARA on 11/22/2010), LEIMS information that has no potential historical or archival value and that does not become part of an investigative file is to be deleted "when the agency determines that it is no longer needed for administrative, legal, audit, or other operational purposes." Understanding that the time frames associated with such purposes can vary widely (*e.g.*, a backup of the database that is overwritten on a nightly basis or a litigation-related preservation order that may remain in effect indefinitely), it is not practical to assign a specific retention period to this type of data. However, it should be understood that the Secret Service has no interest in preserving such information any longer than is absolutely necessary. Estimates of minimum retention times prior to record disposal include five years for generic administrative and laboratory records, 30 years for the storage of occupational hazard exposure records, and indefinite storage for homicide case records, as mentioned above.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in LEIMS will be retained for the timeframes outlined in Section 5.1 to allow the Secret Service to manage, analyze, and distribute evidentiary information regarding threats or potential threats to the safety of individuals, events, and facilities protected by the Secret Service. The retention period is also consistent with general law enforcement system retention schedules and is appropriate given the Secret Service protective and law enforcement missions, as well as the importance of the data required to accomplish its mission.

Section 6.0 Information Sharing

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. PII or summary investigative information maintained in LEIMS may be shared with law enforcement and/or other federal, state, or local government agencies that have official authority and a validated need-to-know the information, and will use the information in a manner consistent with the reason for which it was collected.

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

Any information maintained in LEIMS may be shared in accordance with the purposes and routine uses specified in the DHS/USSS-001 Criminal Investigation Information SORNs in support of the Secret Service's protective and law enforcement missions. The sharing of evidentiary material and reports generated in LEIMS with law enforcement partners is compatible with the purposes of the original collection, which include disclosures reasonable necessary for the purpose of furthering USSS efforts to investigate the activities of and apprehend criminal offenders; developing information on subjects involved in USSS criminal investigations; and assisting other law enforcement agencies in the investigation and prosecution of violations of criminal laws.

6.3 Does the project place limitations on re-dissemination?

Currently, information maintained in LEIMS that is shared with outside law enforcement organizations, and/or other federal, state, or local government agencies is limited to documented investigating officials that have a verified need-to-know. Information may be provided via telephone call, memorandums, reports, facsimiles, and electronic mail. FSD conducts forensic examinations requested by case agents and other law enforcement entities for investigative and judicial purposes. The recipient of results from such forensic examinations is restricted by their applicable local laws, judicial notices, court granted motions, and agency policies as to whom, or if, information related to criminal investigations and activities can be further disseminated. Any SSD Investigatory information that is shared by the USSS is designated for sensitivity as appropriate for a given situation (*e.g.*, Law Enforcement Sensitive, For Official Use Only, Sensitive but Unclassified). If limiting the re-distribution of such information is necessary, the USSS employee that shares the information will ensure that restrictions are communicated to the recipient. Such actions are outside the scope of LEIMS functions and would follow standard DHS/USSS information sharing procedures in compliance with DHS Management Directive 11042.1.

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

Information may be exchanged with other agencies and law enforcement organizations as part of cooperative investigation and response activities. The sharing of investigative information with authorized individuals having a "need-to-know" is not tracked in the LEIMS. The passing of evidence custody to individuals within the USSS and to outside law enforcement organizations, and/or other federal, state, or local government agencies, is recorded to reflect that the items were shared and with whom they were shared. Documentation may occur via a communication log, report, memorandum, or other retained documentation (*e.g.*, Chain of Custody, subpoena, or Motion of Discovery).

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that other agencies may access or disclose the information maintained in LEIMS inappropriately.

Mitigation: The sharing of information described above is only done in accordance with appropriate routine uses and will occur only upon verification of need-to-know and in conjunction with adequate warnings regarding improper re-dissemination. The re-dissemination of LEIMS information is restricted by the receiving law enforcement agency local laws, judicial notices, court granted motions, and agency policies as to whom, or if, information related to criminal investigations and activities can be further disseminated. If limiting the re-distribution of such information is necessary, the USSS employee that shares the information will ensure that restrictions are communicated to the recipient agency. However, such actions are outside the scope of LEIMS functions and would follow standard DHS/USSS information sharing procedures in compliance with DHS Management Directive 11042.1.

Section 7.0 Redress

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

U.S. citizens and Lawful Permanent Residents seeking access to any record containing information maintained within LEIMS, or seeking to contest the accuracy of its content, may submit a Privacy Act (PA) request to the USSS. Individuals, regardless of citizenship or legal status, may also request access to their records under FOIA. Access requests will be directed to the Secret Service's FOIA Officer, Communications Center (FOIA/PA), 245 Murray Lane, Building T-5, Washington, D.C. 20223. Requests will be processed under both FOIA and PA to provide the Requestor with all information that is releasable. Given the nature of the information

in LEIMS, FOIA and PA exemptions may apply and the individual may not be permitted to gain access to, or request amendment of his or her record.

Notwithstanding the applicable exemptions, USSS reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with, or adversely affect the accomplishment of the Secret Service's protective and investigatory mission, information contained within this system may be released or amended. Instructions for filing a FOIA or PA request are available at http://www.dhs.gov/foia.

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

Individuals, regardless of citizenship or legal status, seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the Secret Service's Freedom of Information Act and Privacy Program by mail to Communications Center (FOIA/PA), 245 Murrary Lane, Building T-5, Washington, D.C. 20223.

All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, such requests will be considered on a case-by-case basis consistent with law enforcement necessity.

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

The mechanism for requesting correction of information is specified in the DHS/USSS-001 Criminal Investigation Information SORN, in this PIA, and on the Secret Service's public webpage (www.secretservice.gov/iql_admin.shtml).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may have limited access or ability to correct their information.

Mitigation: This risk is partially mitigated. Individuals can request access to information about them under the FOIA and Privacy Act. Under the Privacy Act, individuals may also request that their information be corrected. The nature of LEIMS and the information it collects and maintains is such that the ability of individuals to access or correct their information may be limited by Privacy Act exemptions. The redress and access measures offered are appropriate given the purpose of the system which is to collect, analyze, process, and store evidentiary and investigative information concerning USSS protective and law enforcement missions.

Section 8.0 Auditing and Accountability

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

All Secret Service 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.

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

All Secret Service employees are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII. In addition, DHS has published the "Handbook for Safeguarding Sensitive PII," which provides employees and contractors additional guidance.

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

DHS physical and information security policies dictate who may access Secret Service computers and filing systems. Specifically, DHS Sensitive Systems Policy Directive 4300A outlines information technology procedures for granting access to Secret Service computers. Access to the information is strictly limited by access controls to those who require it for completion of their official duties.

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?

The LEIMS Operational Managers will review any Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) submitted for the sharing of PII-related LEIMS data. However, the USSS Liaison Division, (which includes the USSS Privacy Office) is the

Primary Office of Responsibility to ensure that an MOU or MOA is appropriate, complete, and reviewed by USSS counsel before being formally accepted by the agency.

Responsible Officials

Latita M. Payne
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.