# Drug Enforcement Administration

**Privacy Impact Assessment**
for the
Laboratory Information Management System (LIMS)

Issued by:
Robert McGovern
DEA Senior Component Official for Privacy (Acting)

Approved by: Kameron Cox
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: October 26, 2026

***(May 2022 template)***

## Section 1: Executive Summary

***Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)***

The Laboratory Information Management Systems (LIMS) is a customized version of a Forensic commercial-off-the-shelf product that falls within the Firebird system boundary.[1] LIMS provides the Office of Forensic Sciences managers with a reliable, accountable system for managing forensic evidence, as well as for overseeing the work of forensic chemists, fingerprint specialists, digital examiners and evidence specialists. The system manages:

- laboratory instrumentation;
- stockpiles and special collections;
- drug and non-drug evidence; and
- case-related documents and information, such as case details reports (CDRs), memorandums, suspect information, chain of custody, results from analysis, report of drug property collected, purchased or seized, etc.

Additionally, LIMS enhances the laboratories' ability to serve as the custodian of all evidence in their possession and supports electronic signatures while creating and maintaining a defensible chain of custody. DEA's Office of Forensic Sciences uses LIMS to carry out its "cradle-to-grave" responsibility for the drug evidence seized by DEA. The investigative nature of evidence analysis may require the laboratory to store personally identifiable information (PII) related to investigations. In particular, the examination of fingerprint evidence has the potential to produce a significant amount of PII.

## Section 2: Purpose and Use of Information Technology.

***2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.***

(a) ***The purpose that the records and/or system are designed to serve and why it is collected.***

LIMS directly supports DEA's core mission by cataloging, tracking, and optimizing the storage of both drug and non-drug evidence (e.g., hard drives, mobile phones, items submitted for fingerprint examination, etc.). LIMS enables DEA laboratories to securely monitor evidence intake, forensic

[1] Firebird is covered by separate privacy compliance documentation.

examiner assignments, and chain of custody. Furthermore, LIMS allows forensic examiners to record the results of their analysis and examination, conduct administrative reviews, and email[2] finalized analysis reports directly to key stakeholders – including law enforcement officials (i.e., Special Agents, Task Force Officers (TFOs), State/Local Officers, etc.), Intelligence Analysts, Diversion Investigators, and prosecutors. Beyond case tracking, LIMS streamlines broader laboratory operations by supporting evidence inventory, materials management, document control, and quality assurance.

LIMS enables DEA laboratories to log evidentiary analysis data while streamlining the forensic support provided to Special Agents, TFOs, Diversion Investigators, the Office of Intelligence, and other law enforcement agencies. LIMS helps the Office of Forensic Sciences manage information more effectively, serving as a cornerstone of their digital, near-paperless workflow.

LIMS has been customized to optimize critical laboratory operations, including tracking evidence containers, managing inventories, capturing and documenting evidence destructions, monitoring evidence released for court proceedings, as well as samples for defense analysis. The system also includes report-view module,[3] fingerprint matrix[4], uncertainty calculator[5], drug picker[6], and reception wizard[7]. LIMS is hosted on DEA's Firebird network[8] and integrates with several other DEA systems, including the Centralized Evidence Reporting and Tracking System (CERTS) within the CONCORDE[9] general support system. Further, Special Agents, Intelligence Analysts, TFOs, and other select users within DEA can correlate laboratory results in LIMS to case-related enforcement and intelligence information via custom Power BI reports that pull data from DEA's Enterprise Data Warehouse (EDW).[10]

***(b) How the information will help achieve DEA's purpose(s):***

The DEA laboratory system supports DEA's core missions through the forensic analysis and examination of seized drug and non-drug evidence. This support also includes the handling and tracking of seized drug evidence from submission to the laboratory system through final disposition in LIMS. The DEA laboratory system includes operations at DEA Headquarters, the Forensic Sciences Training Laboratory in Quantico, Virginia, the Special Testing and Research Laboratory, the INTREPID laboratory, eight (8) regional laboratories, one (1) Digital Evidence Laboratory, and six (6) sub-regional laboratories that provide forensic chemical analysis,

---

[2] All DEA email is encrypted both in transmission and at rest.

[3] Report view module is also known as report distribution in LIMS.

[4] Fingerprint matrix is a worksheet used by friction ridge examiners to document the comprehensive lifecycle of latent print analysis, processing techniques, comparison results and verification milestones for court and discovery purposes.

[5] Worksheet used by forensic chemists to capture all net weight, volume, unit count, and uncertainty calculations.

[6] Drug picker provides the option to view all substances and chemicals available for selection in a LIMS test.

[7] An automated process for accepting evidence into the laboratory.

[8] Firebird is covered by separate privacy documentation.

[9] Both CERTS and CONCORDE are covered by separate privacy documentation (*See* CONCORDE-IMPACT Privacy Impact Assessment and CONCORDE Core Systems Privacy Impact Assessment, respectively).

[10] The EDW is covered by separate privacy documentation for the Enterprise Data Warehouse and Data Management Systems.

fingerprint examination, or digital evidence examination. Forensic examiners further support DEA's core mission by providing expert testimony and field assistance to Federal, state, and local law enforcement personnel.

Primary LIMS users are limited to DEA Forensic Chemists, Fingerprint Specialists, Digital Forensic Examiners, Evidence Specialists, Laboratory Management and Laboratory Administrative personnel.[11] DEA supervisors manage and approve all requests submitted by DEA personnel for LIMS access through DEA's Access Management System (AMS).[12] Users can access, input and retrieve data from LIMS through the DEA Firebird network using single sign-on/Personal Identity Verification (PIV). Therefore, all authorized LIMS users must have a valid Firebird user account. Laboratory and/or friction ridge examination report data can be retrieved via LIMS reports[13] or through Microsoft Power BI reports. DEA and select non-DEA personnel that fall under the DOJ umbrella have access to Microsoft PowerBI dashboards that use data retrieved from EDW. Users of the Microsoft PowerBI dashboards can only see the data displayed; they are not able to access LIMS or it's data directly. Additionally, access to data via EDW does not provide greater access to PII information related to a case than what would be contained in DEA's case management system. The Microsoft PowerBI dashboards are used for administrative and investigative purposes, such as monitoring laboratory performance, tracking substance identification trends, etc.

Laboratory balances[14] and other scientific analytical instruments export data and documents into LIMS via FileShares (either local servers at the lab or AWS Gov Cloud). The data and documents are then picked up by the "Grabber"[15] where they are uploaded into the Scientific Data Management System (SDMS)[16]. LIMS also interfaces with DEA's case management system, the Investigative Management Program and Case Tracking system (IMPACT),[17] and DEA's Centralized Evidence and Reporting Tracking System (CERTS). Other LIMS connections include the Fountain Head system (which receives specific data from LIMS through web services integration), DEA's time and attendance system; DEA's Account Management System (AMS) (for access validation); and EDW (for report writing).

---

[11] Other systems may be used to actually conduct the forensic analysis. For instance, DEA uses LabX software at all of its lab locations to weigh drug and non-drug evidence, friction ridge (fingerprint) analysis is conducted on Authenticated Digital Asset Management System (ADAMS) software, and forensic examinations of seized digital devices are conducted on the Digital Evidence Laboratory Findings Network (SFL9FN). LabX, ADAMS and SFL9FN are covered by separate privacy documents.

[12] AMS is covered by separate privacy documentation.

[13] The term "LIMS reports" refers to administrative reports which differ from the laboratory reports (DEA-113) used to transmit the results of an analysis.

[14] Instrument used to measure the mass of an object.

[15] Grabber is an application that creates a connection channel through which SDMS communicates with other facilities and exchanges data via documents or instrument messages.

[16] SDMS is used to parse data from laboratory instruments into LIMS and auto-populate raw data, charts, and/or graphs into LIMS fields

[17] IMPACT is covered by separate privacy documentation. *See* CONCORDE-IMPACT Privacy Impact Assessment

***2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

| Authority | | Citation/Reference |
|---|---|---|
| X | Statute | 21 U.S.C. § 801 *et seq*, 44 U.S.C § 3101 |
| | Executive Order | |
| X | Federal Regulation | 28 C.F.R. §§ 0.100 and 0.101 |
| | Agreement, memorandum of understanding, or other documented arrangement | |
| | Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology.

***3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.***

LIMS routinely maintains individuals' names and FBI and/or State ID numbers, as well as documents that have been scanned and/or attached to the case record (e.g., DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; results from analysis which includes the Case Details Report and/or Friction Ridge Details Report; DEA-113 Laboratory Report, DEA-111 Friction Ridge Examination Report, etc.). Some of the scanned and/or attached documents may contain aliases, date of birth, addresses, phone numbers, email addresses, and business associates. The only information disseminated by the system is an individual's name and FBI/State ID number as part of the Friction Ridge Examination Report.

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Name | X | A, B, C, and D | Names of members of the public (US or non-USPERs) may be included in LIMS within attachments of DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. Names of employees, contractors, detailees, and other federal government personnel associated with the case (A & B) would be included. |
| Date of birth or age | X | C and D | Date of birth for members of the public (USPER and non-USPER) may appear on documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. |
| Place of birth | X | C and D | Place of birth for members of the public (USPER and non-USPER) appear on documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. |
| Sex | X | A, B, C, and D | Sex of members of the public (USPER and non-USPER) may appear on documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. Possible incidental inclusions for A and B as well. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Race, ethnicity or citizenship | X | C and D | Race, ethnicity or citizenship status for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. |
| Religion | X | C and D | Unlikely, but possible that incidental reference to the religion for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Social Security Number (full, last 4 digits or otherwise truncated) | X | C and D | Social Security Numbers of members of the public (US or non-USPERs) may be included in may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint cards; memorandums; etc. |
| Tax Identification Number (TIN) | X | C and D | Unlikely, but possible that incidental reference to the TIN for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Driver's license | X | C and D | Unlikely, but possible that incidental reference to the driver's license number for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Alien registration number | X | C and D | Unlikely, but possible that incidental reference to the alien registration number for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Passport number | X | C and D | Unlikely, but possible that incidental reference to the passport number for of members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Mother's maiden name | X | C and D | Unlikely but possible that incidental reference to the mother's maiden name may be included may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Vehicle identifiers | X | C and D | Vehicles identifiers for members of the public (C and D) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Personal mailing address | X | C and D | Mailing addresses for members of the public (C and D) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Personal e-mail address | X | A, B, C, and D | Unlikely, but possible that personal email addresses may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. It is also possible that email addresses of DEA employees, contractors, detailees (A) or other GOV personnel (B) may be included in the previously mentioned scanned and/or attached documents. |
| Personal phone number | X | C and D | Personal phone numbers of members of the public (US or non-USPERs) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Medical records number | X | C and D | Potentially, some incidental mention of medical information for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc.. |
| Medical notes or other medical or health information | X | C and D | Potentially, some incidental mention of medical information for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Financial account information | X | C and D | Financial information for members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Applicant information | X | A, B, C and D | Some friction ridge images of applicants including both DEA and other federal personnel, and members of the public (USPER and non-USPER) may be included in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. Further, to the extent applicants that are the subject of DEA investigations may be referenced in the previously mentioned documents. |
| Education records | X | A, B, C, and D | Unlikely, but possible that incidental inclusion of some education information of members of the public (USPER and non-USPER) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. Possible that a CV or other limited education information could be included in court documents with respect to A and B, as attachments. |
| Military status or other information | X | C and D | Military information of members of the public (USPER and non-USPER) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Employment status, history, or similar information | X | A, B, C, and D | Some employment information of members of the public (USPER and non-USPER) could may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. For A and B, employment information such as job title are present in LIMS tables and will appear in court-related attachments such as CVs. |
| Employment performance ratings or other performance information, e.g., performance improvement plan | | | |
| Certificates | X* | A and B* | *Not currently, but future updates to LIMS may include certificates of training records. |
| Legal documents | X | A, B, C, and D | Legal documents related to members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. For A and B, legal documents may appear in documents scanned and/or attached in LIMS, Rule 16; subpoenas; relevant email communication; etc. |
| Device identifiers, e.g., mobile devices | X | C and D | Device identifier information of members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Web uniform resource locator(s) | X | C and D | Web locator information of members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Foreign activities | X | C and D | Foreign activities information of members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Criminal records information, e.g., criminal history, arrests, criminal charges | X | C and D | Criminal records information related to members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation (may contain statements identifying individuals and case numbers); relevant email communication; memorandums; Rule 16; etc. |
| Juvenile criminal records information | X | C and D | Unlikely, but juvenile criminal information of members of the public (US or non-USPERs) may be included if referenced in case or court documents. |
| Civil law enforcement information, e.g., allegations of civil law violations | | | |
| Whistleblower, e.g., tip, complaint or referral | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| Grand jury information | X | C and D | Unlikely, but grand jury information related to subpoenas for LIMS information relevant to members of the public (US or non-USPERs) could possibly be included if it were seeking DEA laboratory work for cases involving those individuals. |
| Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information | X | A, B, C and D | Warrant affidavit by government personnel that includes information about members of the public (US or non-USPERs) who may be witnesses may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc.. |
| Procurement/contracting records | | | |
| Proprietary or business information | X | C and D | Business information of members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; memorandums; etc. |
| Location information, including continuous or intermittent location tracking capabilities | | | |
| *Biometric data:* | | | |
| - Photographs or photographic identifiers | X | C and D | Photographs of members of the public (US or non-USPERs) may be included in LIMS if part of case records. |
| - Video containing biometric data | | | |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - Fingerprints | X | A, B, C and D | Suspect fingerprint biometrics of members of the public (US or non-USPERs) are included in LIMS. Employees, contractors, detailees, and other federal government personnel may also be included if their fingerprints have been identified during the course of examination. |
| - Palm prints | X | A, B, C and D | Suspect biometrics of members of the public (US or non-USPERs) may be included in LIMS. Employees, contractors, detailees, and other federal government personnel may also be included if their palm prints have been identified during the course of examination. |
| - Iris image | | | |
| - Dental profile | | | |
| - Voice recording/signatures | | | |
| - Scars, marks, tattoos | X | C and D | Possible incidental inclusion of such information for members of the public (US or non-USPERs) may appear in documents scanned and/or attached in LIMS, such as DEA-7 Report of Drug Property Collected, Purchased or Seized; DEA-6 Report of Investigation; relevant email communication; fingerprint records; memorandums; etc. |
| - Vascular scan, e.g., palm or finger vein biometric data | | | |
| - DNA profiles | | | |
| - Other (specify) | | | |
| *System admin/audit data:* | | | LIMS maintains audit trails for evidence chain-of-custody functionality. LIMS audit files contain login/logout information of users. |
| - User ID | X | A | As part of LIMS user tables. |
| - User passwords/codes | X | A | As part of LIMS user tables. |
| - IP address | X | A | In LIMS system logs. |

| (1) General Categories of Information that May Be Personally Identifiable | (2)Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<br>A. DOJ/Component Employees, Contractors, and Detailees<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - Date/time of access | X | A | In LIMS system logs. |
| - Queries run | X | A | In LIMS system logs. |
| - Content of files accessed/reviewed | X | A | In LIMS system logs. |
| - Contents of files | | | |
| Other types (please list all other types of identifying information collected and describe as completely as possible): | | | |

### *3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)*

| **Directly from the individual to whom the information pertains: N/A** | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | | Online | |
| Phone | | Email | | | |
| Other (specify): | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Other Federal entities | |
| State, local, tribal | X | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | X | | |
| Other (specify): No agreements exist between the labs and foreign governments per se; DEA's foreign offices submit evidence for analysis on behalf of foreign governments. Laboratory Reports containing the results of analysis are generated and provided back to the submitting Law Enforcement Official. The submitter (e.g. Special Agent, TFO, Officer, etc.) is the party that would track any further dissemination of the report, not the laboratory or LIMS, and would provide these reports under a Mutual Assistance Legal Treaty or some other arrangement. | | | | | |

| **Non-government sources: N/A** | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): | | | | | |

# Section 4: Information Sharing

***4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.***

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Within the Component | X | X | X | LIMS allows batch processing to bulk transfer data within DEA systems (e.g., data transfer to EDW) |
| DOJ Components | X | | | Laboratory reports (DEA-113) and/or Friction Ridge Examination Reports (DEA Form 111) are provided to other DOJ components upon completion of analysis (if such analysis was performed). Additional information such as lab notes, instrumental data, chain of custody info, etc. may be provided to these customers as requested for judicial proceedings, etc. |
| Federal entities | X | | | Laboratory reports (DEA-113) and/or Friction Ridge Examination Reports (DEA Form 111) are provided to other federal entities for evidence that they submitted. Information such as laboratory reports, lab notes, instrumental data, chain of custody info, etc. may be shared for judicial proceedings or for advancement of enforcement cases. |
| State, local, tribal gov't entities | X | | | Laboratory reports (DEA-113) and/or Friction Ridge Examination Reports (DEA Form 111) are provided via encrypted email to external agency customers (such as state/local/tribal agencies) upon completion of analysis. Information such as lab notes, instrumental data, chain of custody info, etc. may be provided to these customers as requested for judicial proceedings, etc. |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | X | | | LIMS data may be shared as part of the evidentiary discovery process and may be presented in a court of law as evidence through counsel. |
| Private sector | | | | |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | **Case-by-case** | **Bulk transfer** | **Direct log-in access** | **Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.** |
| Foreign governments | X | | | Laboratory reports (DEA-113) and/or Friction Ridge Examination Reports (DEA Form 111) are provided back to the DEA submitting agent, who may have submitted evidence on behalf of a foreign government. The submitter would track any further dissemination to foreign governments, not the laboratory or LIMS. Identifying information such as case numbers, defendant names, etc. is redacted unless required based on the circumstance, and Division Counsel or the Office of Chief Counsel can be consulted when the requests seem excessive or exceptional. |
| Foreign entities | X | | | Both foreign governments and foreign entities receive reports of data collected in LIMS, but these reports do not contain case identifying or case specific information nor do they receive actual data from LIMS. Any reports are given to the DEA Special Agent who may disseminate further. |
| Other (specify): | | | | |

***4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.***

Attributable case specific information is not released for Open Data purposes. However, anonymized data resulting from analysis may be made available in public forums at a high level, but the release of any relevant data does not include PII.

## Section 5: Notice, Consent, Access, and Amendment.

***5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.***

This PIA is public information regarding the existence and application of the LIMS system. The system of records notice for the underlying data collected, maintained, and disseminated by LIMS is JUSTICE/DEA-008, "Investigative Reporting and Filing System" 77 Fed. Reg. 21808 (April 11, 2012). This system of records is, however, exempt from the individual notice provisions of the Privacy Act (*see* 28 C.F.R. § 16.98).

***5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.***

Individuals do not have the opportunity to decline to provide information since information is obtained through authorized search authority.

***5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.***

DEA has implemented procedures for individuals to access and amend certain types of information pertaining to them. LIMS data may be shared as part of the Freedom of Information Act (FOIA) or Privacy Act requests, but no private individual or group will be given access to LIMS. FOIA and Privacy Act requests are forwarded from Office of Chief Counsel to the Office of Forensic Sciences, and the office provides data back to Chief Counsel. Chief Counsel reviews any records potentially responsive to FOIA requests on a case-by-case basis to determine whether such records are exempt under FOIA or have been exempted under the Privacy Act.

If subject to prosecution, individuals, through their counsel, will be provided discovery of the DEA's evidence relevant to them. However, people whose communications are intercepted and who are not prosecuted will not gain access to the information in LIMS pertaining to them.

## Section 6: Maintenance of Privacy and Security Controls.

***6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).***

| | |
|---|---|
| X | **The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):**<br><br>LIMS has been granted an ATO and the expiration date is 06/30/2029<br><br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br><br>**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**<br><br>The existing POA&M associated with privacy control is POA&M # 44120. This POA&M requires the development of PIA POA&M will be closed once the PIA is approved. |
| | **This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:** |
| X | **This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:**<br><br>LIMS maintains certain case file information, including laboratory reports, emails, memos, DEA forms, photographs, instrument data, and analyst notes. The provisional impact level for this type of information is MODERATE. If a loss of confidentiality, integrity, or availability regarding this information were to occur, the expected worst-case scenario would be that individuals under investigation may be exposed by the unauthorized disclosure of law enforcement sensitive data to the public, potentially including their fingerprints and laboratory testing results that could lead to reputational damage and possible identity theft. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**<br><br>DEA continuously monitors LIMS for any changes to the system, its operational environment, the information security system and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, updates to the security plan and other relevant documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle.<br><br>DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorization by the DEA Authorizing Official. Significant changes that affect the information system's creation, collection, use, |

| | |
|---|---|
| | processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the Chief Privacy and Civil Liberties Officer (CPCLO), or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement. |
| X | **Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:**<br><br>The application audit logs are reviewed daily as part of the Cybersecurity Operations, Response and Engineering Unit (TCVV) review process. The audit logs are reviewed based off alerting received from Splunk, Crowdstrike, and Vectra (which are Security Information and Event Management tools used for monitoring and audit logging) which occur when an alert is activated.<br><br>The Cybersecurity Operations, Response and Engineering Unit (TCVV) team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts on a daily basis. The DEA Network Operation Center (known as DEACORE) reviews alerts received from Vectra and CrowdStrike that feed into the log management tool and contact the system owner.<br><br>Additionally, the program management office performs weekly reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws. DEACORE is not responsible for dictating the periodic review. The system owner is responsible for complying with all guidelines, policies, and laws; the ISSO for LIMS is responsible for validating that users comply with said governance while the DEA Cybersecurity Operations, Response and Engineering Unit (TCVV enforces actions based upon an infraction (i.e., cybersecurity incidents, policy violations). The Cybersecurity Operations, Response and Engineering Unit (TCVV performs validation for compliance to governance during risk assessments which are scheduled (i.e., ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation. |
| X | **Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.<br><br>Yes, all contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*) and language required listed in each contract awarded within DEA. |
| X | **Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:**<br><br>All DEA Firebird users to include LIMS users, are required to complete Cybersecurity Awareness Training as part of the onboarding process to protect PII. All employees, including contract employees, must complete the training annually. |

***6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

Key Physical Controls: LIMS assets reside in DOJ buildings or GovCloud Servers. LIMS assets are only accessible by vetted approved users[18] in DOJ buildings. Vetted approved users are the only personnel that can access LIMS assets. Physical controls are enforced across all DOJ's buildings as part of its common control requirements. All DEA buildings are guarded by security personnel at the entrance of the office. In addition, employees are required to be authenticated with their Personal Identity Verification card (PIV) before being granted access to the building. Access to LIMS is based on need to know which requires authentication via the PIV card as well.

Key Technical Controls: Security controls, like role-based access control and the identification and authentication controls, are utilized in LIMS. All users are required to access LIMS via their Firebird machine which requires PIV multifactor credential access, the LIMS application is configured to use single sign-on. Access to LIMS is requested via the Account Management System (AMS) and must be approved by the user's supervisor. Thereafter, renewal of a user's LIMS account must be submitted and approved by the user's supervisor every year.

Roles within LIMS vary and the type of information that is accessible depends upon the role of the user. Moreover, DEA and select non-DEA personnel that fall under the DOJ umbrella have access to Microsoft PowerBI dashboards that use LIMS data retrieved from EDW. Users of the Microsoft PowerBI dashboards can only see the data displayed; they are not able to access LIMS or it's data directly. Access to all LIMS electronic records is controlled.

Key Administrative Controls: One of the key administrative controls that is implemented for LIMS is the AT (Awareness and Training) controls. Users of all DEA systems must complete annual DOJ training like Mandatory Records and Information Management (RIM), and Mandatory Cybersecurity Awareness Training (CSAT). This control helps employees understand the importance of security measures, procedures and how to recognize and respond to potential cyber threats. Moreover, LIMS users must read and sign DEA's Information Technology (IT) Rules of Behavior (ROB) to establish accountability, ensure data security and satisfy regulatory compliance upon requesting access. This acknowledgement ensures that the user understands their responsibilities before being granted access to the system. Yearly, at the time of LIMS access renewal, users must re-read and re-sign DEA's IT ROB.

Privacy is analyzed via Assessment and Authorization (A&A) requirements as part of the application of security controls under NIST SP 800-53. Decisions are made based on the need to address private data, such as social security numbers (SSNs) and date of births (DOBs); once the data elements are defined, encryption of those items are included as a database function. All LIMS data at rest is encrypted using AES-256 Customer-Managed Key (CMK)

[18] Vetted approved users include Infrastructure team, DEA Forensic Chemists, Fingerprint Specialists, Digital Forensic Examiners, Evidence Specialists, Laboratory Management and Laboratory Administrative personnel.

technology and data in transit uses an external site-to-site connections provided by the AT&T JUTNet Multiprotocol Label Switching (MPLS) network.

***6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)***

In accordance with the National Archives and Records Administration (NARA), the relevant retention schedule is **"**DEA File No. (DFN) 901-01 (NC1-170-77-1) Laboratory Case Files"[19] which consists of documents pertaining to the analysis of drug and non-drug evidence, evidence accountability and disposition records, chemists worksheets, and related analytical documents. If hardcopies are present, they are transferred to the Federal Records Center 2 years after closing of the investigative case. The records are to be destroyed 10 years after closing of the investigative case. Any LIMS data pertaining to files that are transferred will remain in LIMS. To date, no LIMS data has been purged. Originally, this was because LIMS had only been in existence since 2013, so there was no need to purge any LIMS data until 2023. After 2023, no purge occurred because certain aspects of the LIMS data were needed to analyze and identify drug trends. Currently, there is no way to parse out the data for proper retention of that important information; compliance efforts are ongoing.

Other relevant retention schedules related to data in the case files are:

- DFN 901-03 (N1-170-01-1) Drug Evidence Accountability/Disposition Files — authorization of destruction of evidence records only. After 5 years, destroy record copy after final disposition of drug evidence. After recordkeeping copy has been produced, delete electronic copy; and
- DFN. 901-05 (N1-170-01-1) Latent Fingerprint Program Files are documents related to the administration and operation of the program; exclusive of materials and documents within File No. 901-01 Laboratory Case File. After 6 years, destroy record copy or when it becomes obsolete, superseded, or completely unnecessary for reference, which date is later. Once recordkeeping copy has been produced, delete electronic copy after 180 days; and
- DFN 901-06 (N1-170-01-1), Drug Signature Analysis Files. Record copy is permanently retained. Transferred to National Archives when 15 years old. Copies that are maintained at field laboratories are destroyed after 5 years. Once recordkeeping copy has been produced, delete electronic copy after 180 days.

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether***

[19] DEA Records Information System (DEARIS) Handbook.

***information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

_____ No. _X_____ Yes.

Information pertaining to U.S. citizens and/or aliens lawfully admitted for permanent residence including information from search warrants and/or DEA-6 forms that may be attached to LIMS can be retrieved by searching the LIMS number or IA (Investigative Agency) case and exhibit number.

***7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

Justice/DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf.

## Section 8: Privacy Risks and Mitigation.

***When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?***

### a. Potential Threats Related to Collection of the Information.

**Privacy Risk:** Due to the law enforcement nature of this system, individuals may not consent to or participate in the collection, use, or dissemination of their PII, in most cases.

**Mitigation:** This risk cannot be mitigated in most cases. With respect to the Digital Evidence laboratory within SF, it does receive some exhibits submitted via "Consent", but the submitter (Special Agent/Task Force Officer/Diversion Investigator) will be responsible for notifying the laboratory if, and when such consent is withdrawn. If the consent is withdrawn, the submitter attempts to obtain a search warrant. If a search warrant cannot be obtained, the exhibit is returned to the submitter, and no analysis is performed and any data collected prior to the withdrawal of the consent is not maintained.

For all non-consent evidence that is collected during an investigation and stored in LIMS, it is not feasible nor advisable to provide notice to individuals at the time that their information is stored by the system. The reasoning is because almost all data maintained in LIMS is obtained for law enforcement purposes during the course of active investigations and therefore, the notice requirement is exempted by 28 C.F.R. § 16.98 to the extent LIMS data becomes part of the DEA's Investigative Reporting and Filing System. No individualized notice of laboratory testing is provided, unless individuals are notified through other systems/applications prior to the evidence being entered into LIMS, it is not advisable to

permit individuals to access, correct or amend any PII as the system is used for law enforcement purposes and contains sensitive information related to criminal and civil investigations. DEA maintains a record of LIMS entries to facilitate subsequent discovery notifications in legal proceedings. No notification beforehand can be accommodated due to the risk of compromising ongoing investigations.

**Privacy Risk:** DEA may collect the PII of persons of interest that are relevant to the investigation. Upon completion of forensic examination, it may be determined that the persons of interest do not pertain to the investigation; however, any data provided during the course of the investigation will remain within LIMS. This may increase the number of individuals who may have their information misused or lost in a data breach.

**Mitigation**: This risk is mitigated. LIMS is not used to collect information directly. The decision about which evidence to collect and submit is made by law enforcement officers, either DEA special agents or task force officers, who submit drug and non-drug (fingerprint and digital) evidence to the Office of Forensic Sciences as part of an authorized investigation. The relevance of such evidence to an investigative case must be determined by the investigative team prior to submission to DEA's laboratory. LIMS testing results are kept as a record of the steps DEA took for the investigation.

**b. Potential Threats Related to Use, Access, and Maintenance of the Information**

**Privacy Risk:** DEA may use PII in a manner incompatible/inconsistent with the intended uses or specified purposes for the collection of information.

**Mitigation**: This risk is mitigated. The PII in LIMS was either collected during the course of a criminal investigation or provided by law enforcement officials (e.g., fingerprint cards). There are access controls within LIMS that limit the use of data, as well as accessibility to case-related documents (i.e., laboratory reports, chemists' notes, etc.).

The Cybersecurity Operations, Response and Engineering Unit (TCVV) achieves an application's audit logs to be able to review for suspicious behavior and will notify the security POC of any alerts.

**Privacy Risk:** DEA personnel may access PII within LIMS without a need to know.

**Mitigation**: This risk is mitigated. System auditing tracks activity within LIMS, which uses security controls, like role-based access and identity authentication controls. User access to LIMS must be verified and accepted electronically which will prevent unauthorized access to data at rest. Users are administratively limited to DEA Forensic Chemists, Fingerprint Specialists, Digital Forensic Examiners, Evidence Specialists, Laboratory Management and Laboratory Administrative personnel. Users can access and retrieve data from LIMS via the DEA Firebird network through single sign-on/Personal Identity Verification (PIV). All users must have a valid Firebird user account to access LIMS. Moreover, access is limited to authorized personnel working directly under the Office of Forensic Sciences. Users are further restricted to permission-based role assignments. Access privileges may be extended on a strict need-to-know basis authorized and approved by the office. The data traffic for services and

transportation of data is encrypted using HTTPS.

DEA and select non-DEA personnel that fall under the DOJ umbrella have access to Microsoft Power BI dashboards that use LIMS data retrieved from EDW. Users of the Microsoft Power BI dashboards can only see the data displayed; they are not able to access the LIMS data directly. Access to Microsoft PowerBI dashboards for DEA and non-DEA personnel is granted by the Office of Forensic Sciences personnel, who verify an individual's need to know-similarly to how access is granted to DEA SharePoint sites. Data storage in EDW does not increase PII accessibility, as most authorized personnel already have equivalent access through DEA case management systems. Only select Office of Forensic Sciences users have access to specific EDW datasets or data tables.

**Privacy Risk:** LIMS may retain data longer than necessary, which may reduce the relevance and timeliness of the data.

**Mitigation:** This risk is not mitigated at present. LIMS data is subject to NARA retention schedule, File No. 901-01 (NC1-170-77-1), which specifies: "Transfer case files to Federal Records Center 2 years after close of investigative case. Destroy 10 years after close of investigative case." Due to the inability to parse select data from LIMS to analyze and identify drug trends, no data has been purged. Changes in procedures are underway to conform to LIMS data storage practice with the retention schedule policy.

**Privacy Risk:** The system may be compromised without sufficient physical, technical, and administrative privacy and security controls for handling and protecting PII.

**Mitigation:** This risk is mitigated through a combination of physical, technical, and administrative security controls discussed in Section 6.2. Security and privacy requirements are incorporated into system planning and operations to ensure the protection of PII. Users with LIMS access are required to complete annual DOJ Cybersecurity Awareness Training (CSAT) and comply with established IT ROB for handling PII. Additionally, security and privacy controls are verified and maintained through the Authorization and Accreditation (A&A) process, quarterly Federal Information Security Management Act (FISMA) reviews, annual control assessments, and Continuous Monitoring (ConMon) activities to resolve any deficiencies to increase the security posture and reduce risks.

**Privacy Risk**: DEA personnel may mishandle or fail to protect PII without required and supplemental privacy and security training.

**Mitigation**: This risk is partially mitigated. All DEA Firebird users must complete the following trainings annually: Mandatory Records and Information Management (RIM), National Security Information Classification Guide (NSICG), Insider Threat and Counterintelligence Awareness, Mandatory Cybersecurity Awareness Training (CSAT), and DEA Role-Based Privacy Training. Additionally, users are required to acknowledge and sign IT ROB or their access to IT systems will be revoked. The mandatory annual training and ROB review/acknowledgement reminds all personnel about the use and protection of personally identifiable information.

**Privacy Risk**: Individuals may be unaware of DEA processes to access, amend, and dispute their PII in this system.

**Mitigation**: This risk is mitigated. Individuals may generally be made aware of the opportunity to gain access to information in DEA systems under the guidelines of the Freedom of Information Act (FOIA) public facing website, that contains a "FOIA/Privacy Act (PA)" webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The FOIA/PA website also contains procedures for filing a request for record correction or amendment to DEA.

However, people whose PII are contained in LIMS generally will not gain access to the information in LIMS pertaining to them. By promulgating 28 C.F.R. § 16.98, the Attorney General has made information within LIMS which is part of DEA's Investigative Reporting and Filing System (and other listed systems) exempt from the disclosure, amendment, and correction elements of the Privacy Act pursuant to 5 U.S.C. § 552a(j)(2), (k)(1), and (k)(2). In addition, these records are also complied for law enforcement purposes and thus also may be exempt from production under FOIA 5 U.S.C. § 552(b)(7). With no access to the information in LIMS pertaining to them, individuals cannot request corrections thereto.

### c. Potential Threats Related to Dissemination of the Information

**Privacy Risk:** Privacy risk related to dissemination is disclosure of information to unauthorized persons.

**Mitigation:** This risk is mitigated. All LIMS users have the necessary clearance and agree to comply with the security and dissemination policies and procedures established by DEA. Several security measures exist to prevent both intentional and unintentional unauthorized dissemination, such as: IT monitoring tools, firewalls, intrusion detection, data loss prevention mechanisms, and audit logs. Additionally, transmission of LIMS data occurs only through secure methods, (e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), or Secure Sockets Layer (SSL)) as is consistent with FISMA and NIST security controls. Sharing reports or data from LIMS must comply with DEA policy and relevant SORNs for law enforcement, judicial, or administrative purposes. Additionally, DEA policy mandates that all external dissemination be documented on DEA Form-381. Annually, all DEA personnel are required to take Cybersecurity Awareness Training.