Federal Bureau of Investigation

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

Issued by:
Gregory A. Brower, Privacy and Civil Liberties Officer

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer,
U.S. Department of Justice

Date approved: May 11, 2017

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The Laboratory Information Management System (LIMS) is a Commercial Off the Shelf (COTS) product, with minor customization to include interfaces with STaCSDNA[1] and Sentinel. LIMS provides a database for the Laboratory Division (LD) to describe and track evidence, capture forensic examination procedures and notes, and generate reports of results and conclusions.

LIMS resides on the Lab Division's unclassified Laboratory Network (LABNet[2]) which is a subnet of the FBI's unclassified network (UNet).

A Privacy Impact Assessment (PIA) is required by the E-Government Act.

Section 1: Description of the Information System

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;

LIMS is a configured COTS product used by the LD to track evidence and document its forensic analysis.

(b) the way the system operates to achieve the purpose(s);

Forensic examiners use LIMS to describe the evidence, and record forensic testing results and conclusions. Examination results and conclusions are uploaded to the relevant Sentinel case file and shared with the contributor, i.e., the FBI case agent or other federal, state, local or, via communications through the FBI Legal Attaché (Legat), foreign law enforcement official. There is no further dissemination unless the contributor authorizes sharing with another law enforcement entity, or the sharing is required by a judicial proceeding.

(c) the type of information collected, maintained, used, or disseminated by the system;

The LD receives evidence from crimes under investigation by FBI field offices, and evidence related to violent crimes[3] under investigation by other federal, state, local or, via communications

---

[1] Sample Tracking And Control System for Deoxyribonucleic Acid (STaCSDNA) is a DNA-specific LIMS used by the Laboratory Division DNA Caseworking Unit. STaCSDNA is addressed in separate privacy documentation.

[2] LABNet is addressed in appropriate privacy documentation approved by the FBI Privacy Officer on September 20, 2016.

[3] On a case by case basis at the discretion of the FBI Laboratory Director or designee, the FBI may accept evidence from property crime cases.

through the FBI Legat, foreign law enforcement agencies.

(d) who has access to information in the system;

User groups are established by LD management based on need to know and an appropriate LD role. The user groups are limited to LD personnel, except non-LD FBI technical personnel have access to LIMS to provide "help desk" system support. Data modification privileges are tied to the user's role. In addition, consistent with the Domestic Investigations and Operations Guide, if the nature of the crime or identity of the victim is deemed sensitive, access can be further restricted on a case by case basis. Oversight is provided through the access controls, as well as the ability to audit LABNet for inappropriate access.

(e) how information in the system is retrieved by the user;

Information is user-retrievable within the LIMS by the following data elements, categorized by five data types. Appendix A contains definitions for each data element.

1. **Case-level information**: Lab #, Submitted, Lab, Submission Type, Tracking #, Agency #, Agency, Role, Jurisdiction, Violation, Court, Parties of Interest (First Name, Middle Name, Last Name), Contributor (First Name, Middle Name, Last Name), Business
2. **Parties of Interest**: First Name, Middle Name, Last Name, Alias, Relationship (i.e., subject, victim, missing person, etc.), Date of Birth, Date of Death, UCN (Universal Case Number)
3. **Case Record:** Lab, Unit, Examiner, Discipline #, Status, Exam Type, Case Note Type, Review Type, Review Status, Submitted, Assigned Date, Completed Date, Due Date
4. **Evidence**: Type, Lab, Unit, Examiner, Storage Area, Submitted, By Agency, By Contributor, Received By, Tracking #
5. **Communication Log**:
   - Contact Information: Name, Email, Phone #, Fax #
   - Communication: Type, Date/Time, Message Recipient, Comments, Unit, Entered By, Entered Date
   - Attachments: Attachment Count, Attachment Names

Additionally, management reports, available outside the LIMS on LABNet, can be used to aggregate and search LIMS data for metrics and other LD business needs. Information is user-retrievable through management reports by the following data elements, categorized by six management report types. Note that data elements also available through the LIMS search function are NOT repeated below. Appendix B contains definitions for each management report data element. Management reports are continuously being developed based on LD business needs so the search capabilities are subject to change.

1. **Case Record Management Reports:** Request Coordinator, Activity / Exam Type Description, Agency Type, Reviewer, Review Type, Requester

2. **Configuration Management Reports:** Delegate, User Name / Display Name, Authorization Role, Storage Area / Storage Location
3. **Evidence Management Reports:** Evidence Type, Evidence Agency #, Evidence Description, Transfer Type, Return Method
4. **Proficiency Test Management Reports** (note that access to these reports is limited to select LIMS employees who manage proficiency tests): Test Type, Category, Status, Test ID#, Manufacturer
5. **Resource Manager Management Reports:** Resource Type, Resource, Resource Action, Calibration Period (days)
6. **Submission-Case Management Reports:** Extended Data, Submission Status, Evidence Status, Country

(f) how information is transmitted to and from the system;

Information is manually keyed into LIMS or ingested from Sentinel (case information) through a Sentinel-LIMS interface. Information is transmitted from LIMS via soft copy reports that are uploaded to the FBI's official record system, Sentinel, and hard copy reports that are mailed to all non-FBI contributors.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and

LIMS is accessible via LABNet, to authorized LD employees, contractors, task force members, and detailees. Access is password controlled. LIMS also has interfaces with STaCSDNA and Sentinel.

(h) whether it is a general support system, major application, or other type of system.

Because LIMS provides a systematic means to track evidence and capture forensic test methods and outcomes, it is a critical support system to the FBI's criminal and national security missions.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

LIMS captures two broad categories of information: information that describes evidence, and information that describes testing of the evidence. The latter category includes forensic procedures, standards, controls, instruments, observations, test results, and documents created by the forensic examiner (e.g, charts, graphs, photos) to support the examiner's conclusions.

The information captured in LIMS falls into the five categories described in Section 1(e). LIMS also captures examiner and login identifiers for audit purposes.

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			

Other identifying numbers (specify): None.
Any field marked X indicates that there is a specific LIMS data field designated for this data. Otherwise, LIMS doesn't tag data with identifying numbers. However, the evidence itself may be a document containing these numbers (e.g., a passport, driver's license, pay stub or address book.

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias	X	Home address		Medical information	
Gender		Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	

Other general personal data (specify): None.
Any field marked X indicates that there is a specific LIMS data field designated for this data. Otherwise, LIMS doesn't tag data with these personal identifiers. However, the evidence itself may be a document containing this information.

Work-related data					
Occupation		Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			

Other work-related data (specify): None
Any field marked X indicates that there is a specific LIMS data field designated for this data. Otherwise, LIMS doesn't tag data with work-related identifiers. However, the evidence itself may be a document containing this information.

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	

Other distinguishing features/biometrics (specify): There are no specific LIMS data fields designated for this data; however, photographs or scans of the evidence (or associated paperwork) may contain this information.

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address		Queries run	X	Contents of files	X
Other system/audit data (specify): None.					

Other information (specify)
None.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign	X		
Other (specify): None. The information is evidence related to all crimes under investigation by FBI field offices, and evidence related to violent crimes[4] under investigation by other federal, state, local or, via communications through the FBI Legat, foreign law enforcement agencies. Evidence must be submitted with the relevant case identification numbers and the name of the relevant prosecutor if available.					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): None.					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

[4] On a case by case basis at the discretion of the FBI Laboratory Director or designee, the FBI may accept evidence from property crime cases.

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The information collected is necessary for evidence examination and analysis to support criminal and terrorist investigations. The privacy risks associated with the information provided are the risks of breach and misuse. These risks are minimized by LIMS access and storage security controls:

- [REDACTED TEXT – b7E]
- Login access to the LIMS server is limited to system administrators, who are identified on the LABNet Privileged User list.
- Physical access to the LIMS server is limited to a small number of system administrators (privileged users). Privileged users are listed on the LABNet Privileged User list. [REDACTED TEXT – b7E]
- Privileged users are required to take Privileged User training on an annual basis.
- Remote and mobile access to LIMS is prohibited.
- User groups are established by LD management based on a defined need to know and a role requiring access to the data.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	[ ]	For civil enforcement activities
X	For intelligence activities	[ ]	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	[ ]	To promote information sharing initiatives
[ ]	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	[ ]	For administering human resources programs
X	For litigation		
[ ]	Other (specify): [ ]		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The information is used to conduct forensic examination and analysis of evidence in furtherance of the FBI's law enforcement mission. The Laboratory Division applies scientific capabilities and technical

services to collect, process, and exploit evidence for the FBI and other law enforcement and intelligence agencies. Maintaining this information and disseminating it to authorized individuals allows the FBI Laboratory to support law enforcement and intelligence investigations and ensure casework meets the standards for litigation.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	28 U.S.C. 533
X	Executive Order	E.O. 12333
X	Federal Regulation	28 C.F.R. 0.85
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

The records are currently permanent, pending NARA approval of a proposed 30-year disposition schedule.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.

Privacy risks associated with access to LIMS and the data contained within the database include the possibility of data being mishandled or users viewing data that they are not authorized to view. These risks are mitigated in several ways.

- LIMS is maintained in a physically controlled environment and access is password protected.

- Access to LIMS is limited to LD personnel who have access to a Unet terminal, and access is determined by user role.
- The network supporting LIMS has audit capabilities and is audited weekly for failed logon attempts. The audit features are fully documented in the LABNet System Security Plan (SSP).
- All activity within LIMS is recorded. User accounts are disabled immediately when LD personnel are no longer actively employed by the LD or are found to be using information inappropriately.
- Privileged users are required to take Privileged User training on an annual basis.

PII Confidentiality Risk Level:

☐ **Low** ☑ **Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: [REDACTED TEXT – b7E]
	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements. N/A. Data is obtained directly from the contributor, who in turn is the sole external recipient of the results. There is no collaboration or information sharing as contemplated by this control.
X	Access Control for Mobile Devices: access to PII is prohibited on mobile devices.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access.
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access is prohibited.

Media controls

X	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
	Media Marking: media containing PII is labeled with distribution/handling caveats.
X	Media Storage: media containing PII is securely stored.
	Media Transport: [REDACTED TEXT – b7E]
	Media Sanitation: media is sanitized prior to re-use.
Media (CDs, USBs, etc.) are only used within the LD and are not distributed to anyone outside the LD or to anyone who does not have access to LIMS. Information is not electronically distributed. [REDACTED TEXT – b7E]	

Data Confidentiality controls printed and mailed externally

	Transmission Confidentiality: information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
	Protection of Information at Rest: information stored on a secondary storage device (e.g., hard drive or backup tape) is encrypted. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
Information is not electronically distributed. [REDACTED TEXT – b7E]	

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components	X			

Federal entities	X		[ ]		[ ]		[ ]	
State, local, tribal gov't entities	X		[ ]		[ ]		[ ]	
Public	[ ]		[ ]		[ ]		[ ]	
Private sector	[ ]		[ ]		[ ]		[ ]	
Foreign governments	X		[ ]		[ ]		[ ]	
Foreign entities	[ ]		[ ]		[ ]		[ ]	
Other (specify):	[ ]		[ ]		[ ]		[ ]	

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The privacy risk of improper disclosure of data is the potential of information being misused by individuals who have access to or receive LIMS data. To mitigate the risk, access to LIMS is limited based on the roles assigned for users to accomplish their duties. The roles allow users to view case work that the users are directly supporting. Users do not have access to the entire database. Only system administrators as privileged users can make configuration changes to LIMS. General users do not have the permissions to make configuration changes. In addition, all user activity is recorded for auditing purposes. Prior to gaining access to LIMS, users are cleared by the Laboratory CSO and are required to review and sign the Rules of Behavior (ROB). Lastly, examination results and conclusions are uploaded to the relevant Sentinel case file and only shared with the contributor. There is no further dissemination unless the contributor authorizes sharing with another law enforcement entity, or the sharing is required by a judicial proceeding.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. LIMS does not directly collect information from individuals. Information is collected by contributors pursuant to their investigative authority. However, notice is provided via the published System of Records Notice (SORN), FBI 002, The FBI Central Records System, 63 FR 8659, 671 (Feb. 20, 1998).	
[ ]	Yes, notice is provided by other means.	Specify how: [ ]
	No, notice is not provided.	Specify why not:

5.1 Indicate whether and how individuals have the opportunity to decline to provide information.

[ ]	Yes, individuals have the opportunity to decline to provide information.	Specify how: [ ]
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: LIMS does not directly collect information from individuals. Information is collected by contributors pursuant to their investigative authority. However, information contributed by the FBI is collected pursuant to the Domestic Investigations and Operations Guide (DIOG) and subject to all relevant laws, including, if applicable, the Privacy Act and its consent requirements.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

[ ]	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: [ ]
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: LIMS does not directly collect information from individuals. Information is collected by contributors pursuant to their investigative authority. However, information contributed by the FBI is collected pursuant to the DIOG and subject to all relevant laws, including, if applicable, the Privacy Act and its consent requirements.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and

allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

LIMS does not directly collect information from individuals. Information is collected by contributors pursuant to their investigative authority. However, information contributed by the FBI is collected pursuant to the DIOG and subject to all applicable laws, including, if applicable, the Privacy Act and its consent requirements.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.		
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: LABNet has a current ATO [REDACTED TEXT – b7E]		
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: LIMS conducts quarterly vulnerability assessments and weekly audit log reviews.		
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: LABNet has a current ATO from 14 October 2016.		
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Audit logs are reviewed on a weekly basis. Audit logs include both valid and invalid user log on attempts and any other activity on the network that supports LIMS. LIMS users are validated through Active Directory (AD). General and Privileged user accounts are reviewed annually to validate user access and need to know.		
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.		
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X	General information security training	
	X	Training specific to the system for authorized users within the Department.	
	[ ]	Training specific to the system for authorized users outside of the component.	
		N/A	

	[ ]	Other (specify):	None	

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

The risk of unauthorized access and disclosure is mitigated through LIMS security controls:[5]

- LIMS users are assigned roles. The roles allow users to view only the case work that the users are directly supporting. Users do not have access to the entire database.
- Only system administrators as privileged users can make configuration changes to LIMS. General users do not have permission to make configuration changes.
- Users are required to sign the ROB, thus making them aware of their roles and responsibilities.
- LIMS activity is audited.
- [REDACTED TEXT – b7E]
- Login access to the LIMS server is limited to system administrators, who are identified on the LABNet Privileged User list.
- Privileged Users are required to take the Privileged User training on an annual basis.
- Remote and mobile device access to LIMS is prohibited.
- LIMS user roles are validated on an annual basis.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

[X]	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: FBI 002, The FBI Central Records System, 63 FR 8659, 671 (Feb. 20, 1998) DOJ-002, DOJ Computer Systems Activity & Access Records, 64 FR 73585 (Dec. 30, 1999)
[ ]	Yes, and a system of records notice is in development.
[ ]	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United

[5] The security controls are from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information is user-retrievable within the LIMS by the following data elements, categorized by five data types. Appendix A contains definitions for each data element.

6. **Case-level information**: Lab #, Submitted, Lab, Submission Type, Tracking #, Agency #, Agency, Role, Jurisdiction, Violation, Court, Parties of Interest (First Name, Middle Name, Last Name), Contributor (First Name, Middle Name, Last Name), Business
7. **Parties of Interest**: First Name, Middle Name, Last Name, Alias, Relationship (i.e., subject, victim, missing person, etc.), Date of Birth, Date of Death, UCN (Universal Case Number)
8. **Case Record:** Lab, Unit, Examiner, Discipline #, Status, Exam Type, Case Note Type, Review Type, Review Status, Submitted, Assigned Date, Completed Date, Due Date
9. **Evidence**: Type, Lab, Unit, Examiner, Storage Area, Submitted, By Agency, By Contributor, Received By, Tracking #
10. **Communication Log**:
    - Contact Information: Name, Email, Phone #, Fax #
    - Communication: Type, Date/Time, Message Recipient, Comments, Unit, Entered By, Entered Date
    - Attachments: Attachment Count, Attachment Names

Additionally, management reports, available outside the LIMS on LABNet, can be used to aggregate and search LIMS data for metrics and other LD business needs. Information is user-retrievable through management reports by the following data elements, categorized by six management report types. Note that data elements also available through the LIMS search function are NOT repeated below. Appendix B contains definitions for each management report data element. Management reports are continuously being developed based on LD business needs so the search capabilities are subject to change.

1. **Case Record Management Reports:** Request Coordinator, Activity / Exam Type Description, Agency Type, Reviewer, Review Type, Requester
2. **Configuration Management Reports:** Delegate, User Name / Display Name, Authorization Role, Storage Area / Storage Location
3. **Evidence Management Reports:** Evidence Type, Evidence Agency #, Evidence Description, Transfer Type, Return Method
4. **Proficiency Test Management Reports** (note that access to these reports is limited to select LIMS employees who manage proficiency tests): Test Type, Category, Status, Test ID#, Manufacturer
5. **Resource Manager Management Reports:** Resource Type, Resource, Resource Action, Calibration Period (days)
6. **Submission-Case Management Reports:** Extended Data, Submission Status, Evidence Status, Country

Appendix A

Within LIMS, information is searchable by the following data elements, categorized by five data types.

1. Case-level information

Lab #	LIMS-generated identifier for a Case.
Submitted	Date associated with an instance of providing evidence and request for exam to the Laboratory.
Lab	Within the Laboratory Division, group conducting exams (e.g., Criminal Lab, TEDAC Lab).
Submission Type	Category of evidence submission to include: 1. Forensic Analysis: user-entered submission 2. Proficiency: user-entered submission used by examiners for documenting proficiency tests 3. Sentinel: user-created submission with data elements pre-populated from Sentinel Laboratory Examination Request form 4. Historical: Submission migrated from pre-LIMS Laboratory Division Microsoft Access database
Tracking #	Courier package number associated with evidence receipt (e.g., FedEx tracking number).
Agency #	Agency's file number associated with a submission.
Agency	Name of agency associated with a submission.
Role	Category assigned to agency (e.g., investigating, contributing).
Jurisdiction	Data field not used by LD.
Violation	Offense of the suspected criminal event.
Court	Data field not used by LD.
Parties of Interest (First Name, Middle Name, Last Name)	Person associated to a submission (e.g., subject, victim).
Contributor (First Name, Middle Name, Last Name)	Law enforcement officer associated with a submission.
Business	Business associated to a submission (e.g., subject, victim).

2. Parties of Interest

First Name	First name of person associated with a submission (e.g., subject, victim).
Middle Name	Middle name of person associated with a submission (e.g., subject, victim).
Last Name	Last name of person associated with a submission (e.g., subject, victim).
Alias	Alias of person associated with a submission (e.g., subject, victim).
Relationship	Category assigned to person of interest (e.g., subject, victim, missing person).
Date of Birth	Date of birth of person of interest.
Date of Death	Date of death of person of interest.
UCN	Universal Case Number assigned to person of interest.

3. Case Record

Lab	Within the Laboratory Division, group conducting exams (e.g., Criminal Lab, TEDAC Lab).
Unit	Within the Laboratory Division, forensic discipline conducting exams (e.g., Latent Prints, Trace – hairs/fibers).
Examiner	Name of examiner within the Laboratory Division conducting exams.
Discipline #	Text field with varied use by forensic disciplines, including discipline-specific Case Record status.
Status	Status of Case Record (e.g., exam in progress, complete).
Exam Type	Category of exam requested.
Case Note Type	Category of case note documented.
Review Type	Category of review (e.g., technical, administrative).
Review Status	Status of review (e.g., in progress, completed).
Submitted	Date associated with an instance of providing evidence and request for exam to the Laboratory.
Assigned Date	Date examiner assigned to the Case Record.
Completed Date	Date Case Record completed.
Due Date	Date Case Record due.

4. Evidence

Type	Custody of evidence (i.e., either in a user's personal custody or in a storage area).
Lab	Within the Laboratory Division, group where evidence is located (e.g., Criminal Lab, TEDAC Lab).
Unit	Within the Laboratory Division, forensic discipline where evidence is located (e.g., Latent Prints, Trace – hairs/fibers).
Examiner	Name of examiner within the Laboratory Division with evidence in his/her custody.
Storage Area	Place where the evidence is stored.
Submitted	Date associated with an instance of providing evidence and request for exam to the Laboratory.
By Agency	Name of agency associated with a submission.
By Contributor	Law enforcement officer associated with a submission.
Received By	Name of person within the Laboratory Division who received evidence.
Tracking #	Courier package number associated with evidence receipt (e.g., FedEx tracking number).

5. Communication Log

Contact Information	
Name	Name of person with whom Laboratory employee communicated.
Email	Email address of person with whom Laboratory employee communicated.
Phone #	Phone number of person with whom Laboratory employee

	communicated.
Fax #	Fax number of person with whom Laboratory employee communicated.
Communication	
Type	Category of communication (e.g., received call, left voice message).
Date/Time	User-entered date and time when communication occurred.
Message Recipient	User-entered name of Laboratory employee involved in the communication.
Comments	Documentation of communication.
Unit	Within the Laboratory Division, forensic discipline of person recording communication (e.g., Latent Prints, Trace – hairs/fibers).
Entered By	System-generated name of person within the Laboratory Division who committed Communication Log entry to database.
Entered Date	System-generated date and when communication committed to database.
Attachments	
Attachment Count	Number of attachments associated with a Communication Log entry.
Attachment Names	Name of attachments associated with a Communication Log entry.

Appendix B

LIMS information is searchable through management reports, located on LABNet, using the following data elements. Note that data elements also available through the LIMS search function are NOT repeated below.

1. Case Record Management Reports

Request Coordinator	LD employee who manages Submissions.
Activity / Exam Type Description	Specific type of exam conducted (e.g., hair, firearms, glass, fiber).
Agency Type	Category of agency (e.g., local, Federal, Bureau).
Reviewer	LD employee who conducts reviews of case work.
Review Type	Category of review (e.g., case note review, technical review).
Requester	LD employee requesting a review be conducted on case work.

2. Configuration Management Reports

Delegate	LD employees granted access to perform work on behalf of another employee (e.g., technician performs work on Case Records assigned to an examiner)
User Name / Display Name	LD user/display name used in the LIMS.
Authorization Role	Roles used within the LIMS (FBI Examiner, FBI Clerical User, FBI Supervisor). Each role has an assigned set of permissions (e.g., CanViewCases, CanReceiveEvidence).
Storage Area / Storage Location	Place where evidence is stored.

3. Evidence Management Reports

Evidence Type	Category of evidence (e.g., container, packaging, item, request).
Evidence Agency #	Number assigned to evidence by contributing agency (e.g., FBI assigns 1Bs and barcodes to evidence).
Evidence Description	Text description used to define evidence (e.g., Envelope addressed to Senator Madison).
Transfer Type	Category of transfer (e.g., removed from storage, hand to hand transfer).
Return Method	Category of evidence return (e.g., FedEx, UPS).

4. Proficiency Test Management Reports (note that access to these reports limited to select LIMS employees who manage proficiency tests)

Test Type	Category of test (e.g., external or internal test provider).
Category	Specific type of exam conducted (e.g., hair, toolmarks, firearms).
Status	Status of test (e.g., PT Satisfactory, PT Discontinued).
Test ID#	Number assigned to test.
Manufacturer	Test provider.

5. Resource Manager Management Reports

Resource Type	High-level organization of Resource Instances (e.g., instruments, pipettes, microscopes).
Resource	Low-level category for Resource Instances (e.g., mass spectrometry, spectroscopy).
Resource Action	A task performed on a Resource Instance (e.g., calibration, maintenance).
Calibration Period (days)	Cycle of calibration for Resource Instances.

6. Submission-Case Management Reports

Extended Data	Category of case (e.g., Indian Country Case, Major Case).
Submission Status	Status of submission (e.g., closed, in progress).
Evidence Status	Status of evidence (e.g., personal custody, returned to agency).
Country	Country where violation occurred.