

Date of Approval: **March 09, 2023**

PIA ID Number: **4396**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Laboratory Information Management System, LIMS

Is this a new system?

No

Is there a PCLIA for this system?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

None needed

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The LIMS application is a component of the CI-1 GSS environment that resides in the Center for Science and Design (CSD). It is used to track evidence, issue analytical results, manage examination documentation, and integrate quality management processes. There are neither internal system connections within or outside the CI-1 boundary, nor external system connections outside the IRS network. Only CI users have access to the LIMS component. PII & SBU data are manually entered by CI users. The information is imported into reports for the requesting agents or laboratory customers. Additional information includes, Form 13437 (Evidence Request) is used and uploaded into LIMS (JusticeTrax).

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

Laboratory receives fraudulent tax forms in investigations. During the course of examination these forms are scanned, and the SSN appears in the image. SSNs are not entered in as numbers in a database field.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

We do not use SSN for any purpose other than they appear in our scans of documents. There is no way to avoid this.

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing Address
Phone Numbers
E-mail Address

Date of Birth
Biometric Identifiers
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Official Use Only (OUO) or Limited Official Use (LOU) - Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Criminal Investigation Information - Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Information by CI for certain money laundering cases may be 18 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

SSNs are not used for any purpose. The site has mainly evidence, issue analytical results, and manage examination documentation.

How is the SBU/PII verified for accuracy, timeliness, and completion?

Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information includes individual citizen's social security numbers, names, dates of birth, places of birth, parents' names, etc.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

- IRS 46.002 Criminal Investigation Management Information System and Case Files
- IRS 46.003 Confidential Informants
- IRS 46.005 Electronic Surveillance and Monitoring Records
- IRS 46.015 Relocated Witnesses
- IRS 46.050 Automated Information Analysis System

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

No

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: F13437

Form Name: Evidence Request

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Department of Treasury

Transmission Method: Authenticate users via web-based systems

ISA/MOU: No

Identify the authority.

5 U.S.C. 301, 31 U.S.C. 5311-5332, 26 U.S.C. 7801, and Department of the Treasury Delegation Orders and Directives authorizing CI to conduct investigations into specified non-tax crimes.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Material covered by rule 6(e) of the Federal Rules of Criminal Procedure may be disclosed only as permitted by that rule.

For what purpose?

Results of forensic analysis.

Does this system disseminate SBU/PII to State and local agencies?

Yes

Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: State Agencies
Transmission Method: Electronic Transmission
ISA/MOU: No

Identify the authority.

Federal agencies that offer online government services to secure the privacy of citizens, businesses, and other government agencies. 5 U.S.C. 301, 31 U.S.C. 5311-5332, 26 U.S.C. 7801, and Department of the Treasury Delegation Orders and Directives authorizing CI to conduct investigations into specified non-tax crimes.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Material covered by rule 6(e) of the Federal Rules of Criminal Procedure may be disclosed only as permitted by that rule. Disclose information to Federal, state, local, tribal, and foreign law enforcement and regulatory agencies regarding violations or possible violations of Bank Secrecy Act, money laundering, tax, and other financial laws when relevant and necessary to obtain information for an investigation or enforcement activity.

For what purpose?

Results of forensic analysis.

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Information is supplied by law enforcement personnel pursuant to criminal investigations.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Legal investigation supports activities associated with gathering information about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

Central Records and Statistics Management involves the operations surrounding the management of official documents, statistics, and records for the entire Federal Government. Due process would be contained in these records. This information type is intended to include information and information systems associated with the management of records and statistics for the Federal government as a whole, such as the records management performed by NARA, or the statistics and data collection performed by the Bureau of the Census.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

How is access to SBU/PII determined and by whom?

Access to LIMS is ultimately approved by the Laboratory Director. Approval is granted and monitored through BEARS.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

5/1/2022

Describe the system's audit trail.

IT Security Specialists are required to review audit information including audit trail reviews after an event as well as hold scheduled audit reviews at least weekly - or more frequently at the discretion of the information system owner. However, when suspicious or inappropriate behavior is suspected, security personnel will review the applicable reports and logs for evidence of the activity and report findings to an appropriate manager for further action.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

For the LIMS application, corrective measures are applied and tested prior to installation.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

No