

Date of Approval: **June 21, 2023**

PIA ID Number: **7810**

SYSTEM DESCRIPTION

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

LB&I Taxpayer Registry, LTR

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

LB&I Taxpayer Registry, LTR, 5836

What is the approval date of the most recent PCLIA?

3/1/2021

Changes that occurred to require this update:

Significant System Management Changes

Were there other system changes not listed above?

No

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

Under: The Cloud Governance Board (CGB), the Enterprise Operations Governance Board (EOPs GB), and the UNS Technical Integration Board (TIB). 933538381404010000 (35-38-G1E41) Information Technology Enterprise Operations Technology Implementation Svcs Tech Deployment Svcs Ofc Infrass Upgrade Svcs Sec ECC, CCB & IMCCB

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?

Yes

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 Large Business & International (LB&I) Taxpayer Registry (LTR) is a collaborative application built on Microsoft SharePoint and SQL (Structure Query Language) Server technology. Prior to SharePoint Online, which is in the cloud, the LTR's applications used SharePoint 2013 which is on premises software/storage. The LTR applications also used out of the box SharePoint software/capabilities such as Business Connectivity Services, Nintex, and SQL Server Reporting Services along with service accounts to obtain/display data from its database and capture/store data from users. With the standup of SharePoint Online, significant system management changes include moving to the cloud and none of the existing software/capabilities being available. In its place is a dedicated environment, which the LTR has requested and received. Along with the dedicated environment is a data gateway for use with the Power Platform tools to connect to its on-premise SQL database. While the LTR applications generally do not store data on SharePoint, the way its applications connect to the SQL database has changed. LTR, developed and maintained by LB&I, is used for multiple strategic LB&I compliance initiatives including campaigns, Schedule UTP (Uncertain Tax Positions), Office of Tax Shelter Analysis (OTSA), and other projects such as Large Partnership Compliance, Partnership Model, Foreign Payments Practice, and Research Risk Review. LTR collates data from multiple existing systems to enable the filtering, classification, risk assessment, feedback, and reporting of taxpayer compliance for the LB&I population to various stakeholders e.g., management, analysts, technical specialists, and the field. Data is periodically extracted, transformed, and loaded into LTR to enable the matching of published financial information with tax filing information, identification and analysis of compliance issues and reporting. Information is delivered to the field and feedback gathered from the field to improve upstream processes. The LTR development and testing will occur in the pre-production environment (DSTEST) and deployed into the production environment (DS) using the IRS Information Technology (IT) Enterprise Architecture One Software Development Life Cycle (One SDLC) process. The LTR uses SharePoint as a front-end vehicle to extract data stored in SQL databases and then display the data meeting the needs of various users. For example, data is extracted for a specific taxpayer and displayed on the LTR's Company Profile Report. Users use this information for Risk Assessment purposes in conjunction with other systems, such as the Content Management & Collaboration (CMC) system and Issue Management System (IMS). Data from the LTR is not sent to the CMC or IMS at this time. Another example is displaying the data in a dashboard for reporting purposes. Most reported data is aggregated in reports created using the Power BI Platform and connecting to LTR's SQL database using a data gateway. Users will either input or view information that has been input or made available via SharePoint or the Power Platform. Users input information either as part of a specific project or program, or as part of the Feedback Process. The Company Profile Report is an accumulation of historical and current taxpayer data available to assist with the classification and risk analysis

of LB&I taxpayers in one central location. Additionally, the LTR collects feedback for various LBI initiatives. Using the appropriate feedback entry point on the LTR, the user will input their feedback information into a browser-based form. Information from the following data sources is linked and stored in the LTR database: Internal Tax Information: 1) LB&I Datamart (Modernized e-File (MeF), Business Return Transaction File (BRTF), Schedule K-1, TC 590, Data Capture System (DCS), Compliance Data Warehouse (CDW), Audit Information Management System (AIMS)) 2) IBMIS (Issue Based Management Information System) 3) IMS (Issue Management System) 4) OTSA (Office of Tax Shelter Analysis) 5) SWC (Selection and Workload Classification) 6) LB&I CMC (Content Management & Collaboration) 7) LB&I CBF (Case Built File) 8) LB&I TIG (Taxpayer Information Gateway) 9) LIN (LB&I Image Network) 10) ERCS (Examination Returns Control System) 11) EOAD (Examination Operational Automation Database) External Financial Information.

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:

Legal/statutory basis (e.g., where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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

SSNs are used to identify taxpayer data for statistical research and information gathering focusing on campaigns, not individual taxpayer(s).

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

None. The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The LB&I Taxpayer Registry requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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
Standard Employee Identifier (SEID)
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.

Proprietary Data - Business information that does not belong to the IRS.

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

PII for personnel administration is 5 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.

SBU data is required for the risk assessment and analysis by LB&I staff to identify returns for examination, provide feedback for management analysis, for Subject Matter Experts to review compliance trends, and for analysts and management to manage various programs and projects. PII data, such as SSNs, are sometimes required for specific LB&I projects and purposes. Additionally, SSNs associated with filings such as Forms 1065 and 1120S are required as part of the filing. These taxpayers file Schedule K-1 with their forms to identify the partner/shareholder of the filer which may be an individual taxpayer with an SSN. These SSNs or their equivalent may be stored in a retrievable format, such as through a database query and made available to classifiers and the field via the LTR Company Profile. When a user searches for a Taxpayer Identification Number (TIN) in the system, it is logged, and the Negative TIN (NTIN) service call is activated to obtain the users' list of associated NTINs. Additionally, when user clicks on a related TIN link, the NTIN service call is activated. If user's Standard Employee Identifier (SEID) is associated with the TIN in the NTIN list, the user will receive a message and no data will be displayed. The NTIN service call will run nightly at least once every 24 hours to update associated NTINs. In addition, a small number of SSNs are sometimes disclosed by some taxpayers on their tax filings and disclosures on a limited basis on some forms and may be contained in documents stored and accessed through the LTR. This incidental use of SSNs by LB&I taxpayers makes viewing of some SSNs by authorized users unavoidable and necessary. Internal Revenue Code section 6109 is the authority that allows the use of SSNs. These SSNs, not used by a specific project, may still be potentially searched via SharePoint text search by research analysts with authorized access and viewed by examiners assigned to the case when they view the pdf forms. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. LB&I also has many campaigns that involve individual taxpayers with SSNs. In order to provide feedback, SSNs are used in the LTR Feedback Tool to identify the specific taxpayer to which feedback is being provided. Users are allowed access to the appropriate feedback questionnaires based on their assignment of the taxpayer, which has been determined earlier on in the examination process.

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

LTR aggregates SBU/PII data from other internal IRS sources, which have their own data cleansing and validation processes. Consequently, LTR does not do any independent updates to the SBU/PII data. It does verify that the data has been transferred correctly between systems. This verification is done by the LTR developers. Non-IRS sourced data (Example: SEC Financial Information) is initially reviewed by transcribers. For example, transcription errors for SEC information are corrected when the errors are detected. Then an additional review for accuracy is performed by Subject Matter Experts (SME) before inclusion in the LTR.

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 42.021 Compliance Programs and Projects Files

IRS 42.001 Examination Administrative Files

IRS 42.008 Audit Information Management System

IRS 34.037 Audit Trail and Security Records

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?

Yes

Enter the files and databases:

System Name: IBMIS
Current PCLIA: No
SA&A: No

System Name: AIMS
Current PCLIA: No
SA&A: No

System Name: ERCS
Current PCLIA: No
SA&A: No

System Name: CMC
Current PCLIA: No
SA&A: No

System Name: CBF
Current PCLIA: No
SA&A: No

System Name: LB&I Workload Identification System (LWIS)
Current PCLIA: No
SA&A: No

System Name: Securities and Exchange Commission (SEC)
Current PCLIA: No
SA&A: 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: 1041

Form Name: Form 1041 U.S. Income Tax Return for Estates and Trusts

Form Number: 1042

Form Name: Form 1042 Annual Withholding Tax Return for U.S. Source Income of Foreign Persons

Form Number: 1065

Form Name: Form 1065 U.S. Return of Partnership Income

Form Number: 1065B

Form Name: Form 1065 Schedule B-1 Information on Partners Owning 50% or More of the Partnership

Form Number: 1066

Form Name: Form 1066 U.S. Real Estate Mortgage Investment Conduit (REMIC) Income Tax Return

Form Number: 1120

Form Name: Form 1120 U.S. Corporation Income Tax Return

Form Number: 1120C

Form Name: Form 1120-C Form 1120-C, U.S. Income Tax Return for Cooperative Associations

Form Number: 1120F

Form Name: Form 1120-F U.S. Income Tax Return of a Foreign Corporation

Form Number: 1120FSC

Form Name: Form 1120-FSC U.S. Income Tax Return of a Foreign Sales Corporation

Form Number: 1120L

Form Name: Form 1120-L U.S. Life Insurance Company Income Tax Return

Form Number: 1120PC

Form Name: Form 1120-PC U.S. Property and Casualty Insurance Company Income Tax Return

Form Number: 1120R

Form Name: Form 1120-REIT U.S. Income Tax Return for Real Estate Investment Trusts |
Form 1120-RIC U.S. Income

Form Number: 1120S

Form Name: Form 1120-S U.S. Income Tax Return for an S Corporation

Form Number: 720

Form Name: Form 720 Quarterly Federal Excise Tax Return

Form Number: 8804

Form Name: Form 8804 Annual Return for Partnership Withholding Tax (Section 1446)

Form Number: 945

Form Name: Form 945 Annual Return of Withheld Federal Income Tax

Form Number: 945A

Form Name: Form 945-A Annual Record of Federal Tax Liability

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

8/5/2022

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Any individual tax information is received from a system that provides taxpayers with notice and rights to consent and/or amend, as needed, according to various IRCs, through notifications such as Publication 1. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

The entire process and procedures are dictated by the Internal Revenue Manual guidelines - IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations per the appeals process.

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

Data access is granted on a need-to-know basis. A potential user must submit a request for access via IRS Business Entitlement Access Request System (BEARS) to their local management for approval consideration. Users are not permitted access without BEARS access from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined in BEARS and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access.

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 Only

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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

Access to the LTR is restricted based upon an individual's role through a combination of BEARS applications, SharePoint permission controls, CBF case assignment and IMS team membership.

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?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records housed in the LTR system will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 23 item 86, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Monthly reviews, in accordance with IRM 10.8.1.4.16.14.1.1., of access lists is performed, logged, and maintained by the application system administration staff for later inspection and audit purposes.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

We have a sandbox and Test environment. We will roll out changes, through change promotion.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

4/27/2020

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: More than 100,000

Contractors: More than 10,000

Members of the Public: Not Applicable

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