Date of Approval: **May 26, 2021**

PIA ID Number: **5791**

SYSTEM DESCRIPTION

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

Lead and Case Analytics, LCA

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?

Lead and Case Analytics, LCA PIA ID Number: 3179

What is the approval date of the most recent PCLIA?

1/10/2018

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Expiring PCLIA

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.

CIGB Criminal Investigation Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

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.

LCA is an enterprise-wide, single-platform data analytic service that leverages the Palantir Gotham ("Gotham") and Foundry platforms to provide the capability for seamless research and analysis in one unified environment. Today's sophisticated financial schemes to defraud the government demand the technology to compile disparate case data and the analytical tools to wade through complex financial records to identify fraudulent activity. Special agents and investigative analysts (IAs) in Criminal Investigation (CI) utilize the platform to find, analyze, and visualize connections between disparate sets of data to generate leads, identify schemes, uncover tax fraud, and conduct money laundering and forfeiture investigative activities. Each application is integrated seamlessly with others, allowing users to perform multi-faceted investigations without leaving the LCA platform. LCA's data integration technologies enable organizations to access all their data from a single workspace, regardless of the size of the data or format.

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:

When there is no reasonable alternative means for meeting business requirements

Law enforcement and intelligence purposes

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

LCA uses the SSNs to identify taxpayers along with spouses and dependents.

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

The Office of Management and Budget Circular A-130 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. Lead and Case Analytics requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer 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
Place of Birth
Mother's Maiden Name
Internet Protocol Address (IP Address)
Criminal History
Passport Number
Financial Account Numbers
Tax Account Information
Centralized Authorization File (CAF)

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.

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

PII about individuals for Bank Secrecy Act compliance 31 USC

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.

LCA/Palantir is used to examine information & patterns of suspicious activities that will determine if a case should be created for further follow up. SBU & PII information is used in the Agent's analysis. SSN, Contact Information (name, address, phone numbers, Date of Birth (DOB), and IP addresses) are used to identify individuals directly and indirectly related to the investigation. Viewing Financial Account numbers, and Tax Account Information and retrieving Passport Numbers (to gather travel tendencies) also helps in identifying fraud, ID

theft or tax evasion. Gathering Criminal History on individuals related to the investigation provides the Agents with information on those individuals which may be contacted by the Agent. Without access to this information an AI or Agent could not complete its duty to fully investigate potential criminal activity.

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

The accuracy, completeness, validity, and authenticity are done at the application-level. Both the source & project validate input via the application software. The information input into the LCA repository is already edited by applications utilized by CI. When information from source systems is ingested, it is translated into a Palantir Extensible Markup Language, (PXML) format that maps to a Palantir-specific schema called ontology. The ontology contains the definition of all entities, documents, properties and links that are abstracted from the underlying data. The ontology itself is created by iterating with end users to create representations that make sense and have value. Ontologies are not permanent and can be changed to improve end user experience. Entities, documents and links all can be assigned properties. These properties can represent a single value or a composite property that represents multiple components (e.g. Address property may represent a street address, city, state and ZIP Code). Entities, documents and links can only be assigned properties that are flagged as being allowed in the ontology. Values mapped to ontology properties are parsed from the raw data and can be restricted by type and format. For example, SSN's should contain non-numeric characters. In the event that a value does not match the proper type or format, the value turns red to acknowledge the unexpected format. Access Control Lists (ACL) can be used to restrict access (read, write, discover, owner) at the granularity of a single property value. End users can only query and see items they are permitted to see through the ACL. It's important to note that an end user with write permissions on a particular data set cannot add properties that are unauthorized by the definition of the ontology. For example, an end user with write permissions cannot add a Filing Date property to a Location entity but may assign an Address property.

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 46.050 Automated Information Analysis System

IRS 42.021 Compliance Programs and Projects Files

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: RRP Application (Return Review Program)
Current PCLIA: Yes
Approval Date: 12/6/2019
SA&A: Yes
ATO/IATO Date: 6/21/2019

System Name: IPM Application (Integrated Production Model)
Current PCLIA: Yes
Approval Date: 6/6/2019
SA&A: Yes
ATO/IATO Date: 4/1/2015

System Name: Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 5/29/2018

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

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: SBA (Small Business Administration
Transmission Method: Electronic File Transfer Utility (EFTU)
ISA/MOU: Yes

Name: FinCen
Transmission Method: Electronic File Transfer Utility (EFTU)
ISA/MOU: Yes

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: Schedule A (Form 1040)
Form Name: Itemized Deductions

Form Number: Form 1040
Form Name: U.S. Individual Income Tax Return

Form Number: Schedule C (Form 1040)
Form Name: Profit or Loss From Business

Form Number: Schedule EIC (Form 1040A or 1040)
Form Name: Earned Income Credit

Form Number: Schedule F (Form 1040)
Form Name: Profit or Loss From Farming

Form Number: Form 8888
Form Name: Allocation of Refund (Including Savings Bond Purchases)

Form Number: Form W-2
Form Name: Wage and Tax Statement

Form Number: Form 1098
Form Name: Mortgage Interest Statement

Form Number: Form 1099G
Form Name: Certain Government Payments

Form Number: Form 1099MISC
Form Name: Miscellaneous Income

Form Number: Form 1041 K1
Form Name: U.S. Income Tax Return for Estates and Trusts

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

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

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

Form Number: Form 943
Form Name: Employer's Annual Federal Tax Return for Agricultural Employees

Form Number: Form 941
Form Name: Employer's Quarterly Federal Tax Return

Form Number: Form 940
Form Name: Employer's Annual Federal Unemployment (FUTA) Tax Return

Form Number: Form 720
Form Name: Quarterly Federal Excise Tax Return

Form Number: Form W-7
Form Name: Application for IRS Taxpayer Identification Number

Form Number: Form SS4
Form Name: Application for Employer Identification Number

Form Number: Form 1098C
Form Name: Contributions of Motor Vehicles, Boats and Airplanes

Form Number: Form 1098T
Form Name: Tuition Statement

Form Number: Form 1099DIV
Form Name: Dividends and Distributions

Form Number: Form 1099INT
Form Name: Interest Income

Form Number: Form 1099K
Form Name: Payment card and Third Party Network Transactions

Form Number: Form 1099OID
Form Name: Original Issue Discount

Form Number: Form 1099R
Form Name: Distributions from Pensions, Annuities, Retirement or Profit-Sharing Plans

Form Number: Form 1099S
Form Name: Proceeds from Real Estate Transactions

Form Number: Form 1099SA
Form Name: Distributions from an HSA, Archer MSA, Medicare Advantage MSA and HSA

Form Number: Form5498
Form Name: IRA Contribution Information (info copy only)

Form Number: Form 8805
Form Name: Foreign Partner's Information Statement of Section 1446 Withholding Tax

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?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Splunk
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: Yes
ATO/IATO Date: 3/28/2017

Identify the authority.

5 U.S.C 301, 1302, 2951, 4118, 4308 and 4506 18 U.S.C. 1030 (a)(2)(B) 26 U.S.C. 7801 Executive Orders 9397 and 10561.

For what purpose?

To maintain records of individual and business tax returns, return transactions and authorized taxpayers. To identify and track any unauthorized accesses to sensitive but classified information and potential breaches or unauthorized disclosures of such information.

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

No

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

No

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?

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?

The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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

No

Why not?

The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

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

The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

INFORMATION PROTECTION

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

Contractor Owned and Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

Access to the Lead and Case Analytics (LCA) analytic service is requested via Online BEARS. Access is granted on a need-to-know basis. The BEARS enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is performed through the OL5081.

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 LCA 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 Schedules (RCS) 30 for Criminal Investigation, Item 15 for Case Files, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Per IRM 10.8.1.4.16.6

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?

4/30/2021

Describe the system's audit trail.

Leveraging LCA knowledge management technologies, LCA's auditing model protects privacy and civil liberties by providing data transparency, immutable audit trails, and fine-grained security controls. Audit trials include information about each time data is viewed, tagged, or exported - including by whom and the time of the specific activity that occurred. Further, by default, LCA will log any changes to data, the user who instituted those changes and the time of those changes. Users who lack the ability to modify objects will not be allowed to modify them. LCA also logs other user actions including logins, searches, and user group changes, among other parameters.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

The results are stored in DocIT (Document Management System)

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Communicated the overall test strategy, dependencies, risks, schedules, and roles and responsibilities to the testing team and the business project stakeholders. - Determined whether a system had passed or failed a requirement. Unique Test Cases are built consisting of information such as test conditions, test data, test steps, verification steps, prerequisites, results/outputs, pass/fail rating and test environment. User Acceptance Test (UAT) is conducted with the end-users & signed off as acceptable - An End of Testing report, was created, including a summary of the testing objective, approach, test schedule, and test environment. It provides details about the test execution, including test team members, test cases, test summary, and test results. It also identifies the defects found, including a defect report summary and disposition of the defects. The test exit criteria indicates whether testing can be considered completed. The test exit criteria for the LCA system include: All test cases have been successfully executed as documented; if not, test cases are placed on the Product Backlog or Defect Backlog or waived with appropriate approval Unresolved defects have been negotiated and the schedule has been updated for defect remediation.

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: Under 50,000

Contractors: Under 5,000

Members of the Public: More than 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