Date of Approval: February 14, 2018 PIA ID Number: **3179**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Lead and Case Analytics (LCA), LCA, LCA

2. Is this a new system? No

2a. If no, is there a PIA for this system? Yes

If yes, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Lead Case Analysis, PIAMS # 1120

Next, enter the date of the most recent PIA. 07/28/2017

Indicate which of the following changes occurred to require this update (check all that apply).

Yes	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
Yes	Preliminary Design/Milestone 3
Yes	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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") platform 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, undercover 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If 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

If yes, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If yes, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

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 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. 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.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If yes, specify the information.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
No	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If yes, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of

		property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

If yes, describe the other types of SBU/PII that are applicable to this system.

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
Yes	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

If the answer to 6f is no, verify the authority is correct with the system owner and then update the answer to 6f.

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

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.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If yes, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If yes, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If no, explain why the system does not have a SORN?

If other**,** explain your answer**.**

If yes, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	**SORNS Name**
IRS 46.050	Automated Information Analysis System
IRS 46.009	Centralized Processing & Evaluation of Information
IRS 42.021	Special Projects and Program Files
IRS 34.037	Audit Trail and Security Records System

If yes, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ##Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Electronic Fraud Detection System (EFDS) Preparer Tables	Yes	10/24/2014	Yes	01/15/2015
EFDS Electronic Filing (ELF) 8888	Yes	10/24/2014	Yes	01/15/2015
EFDS Return Misc Tables	Yes	10/24/2014	Yes	01/15/2015
EFDS SchA Tables	Yes	10/24/2014	Yes	01/15/2015
EFDS SchC Tables	Yes	10/24/2014	Yes	01/15/2015
EFDS Prison/er Tables	Yes	10/24/2014	Yes	01/15/2015
EFDS Business Master File (BMF) Tables	Yes	10/24/2014	Yes	01/15/2015
Unified Suspicious Actvity Report (SAR) Financial Crime Enforcement Network (FinCEN) Business SAR (BSAR)	Yes	10/24/2014	Yes	01/15/2015
Unified Currency Transaction Report (FinCEN) (UCTR)	Yes	10/24/2014	Yes	01/15/2015
Currency Transaction Report (FinCEN) (CTR)	Yes	10/24/2014	Yes	01/15/2015
Suspicious Activity Report – Depository Institution (FinCEN) (SAR-DI)	Yes	10/24/2014	Yes	01/15/2015
Suspicious Activity Report – Casino (FinCEN) (SAR-C)	Yes	10/24/2014	Yes	01/15/2015
Suspicious Activity Report – Money Service Business (FinCEN) (SAR-MSB)	Yes	10/24/2014	Yes	01/15/2015
Suspicious Activity Report – Securities and Features (FinCEN) (SAR-SF)	Yes	10/24/2014	Yes	01/15/2015
Report of Cash Payments Over $10,000 Received in Trade or Business (FinCEN) Form 8300	Yes	10/24/2014	Yes	01/15/2015
EFDS ELF W2	Yes	10/24/2014	Yes	01/15/2015
EFDS STARS Tables	Yes	10/24/2014	Yes	01/15/2015
W-7 Tables	Yes	10/24/2014	Yes	01/15/2015
BSTARS Table	Yes	10/24/2014	Yes	01/15/2015
Report of International Transportation of Currency or Monetary Instruments (FinCEN) (CMIR)	Yes	10/24/2014	Yes	01/15/2015
Report of Foreign Bank and Financial Accounts (FinCEN) (FBAR)	Yes	10/24/2014	Yes	01/15/2015

Report of Foreign Bank and Financial Accounts (FinCEN) (FFBAR)	Yes	10/24/2014	Yes	01/05/2015
Registration of Money Service Business (FinCEN) (RMSB)	Yes	10/24/2014	Yes	01/15/2015
Information Return Master File (IRMF) 1098 Mortgage Interest Statement	Yes	10/24/2014	Yes	01/15/2015
IRMF 1099 MISC Miscellaneous Income	Yes	10/24/2014	Yes	01/15/2015
IRMF W2 Wage & Tax Statement	Yes	10/24/2014	Yes	01/15/2015
EFDS Returns	Yes	10/24/2014	Yes	01/15/2015
EFDS ELF Summary	Yes	10/24/2014	Yes	01/15/2015
EFDS Dependents	Yes	10/24/2014	Yes	01/15/2015
EFDS In Process Returns	Yes	10/24/2014	Yes	01/15/2015
EFDS MISC Returns	Yes	10/24/2014	Yes	01/15/2015

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If 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).

Organization Name	Transmission method	ISA/MOU
FinCen	Electronic File Transfer Utility (EFTU)	Yes

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from Taxpayer forms? Yes

If yes, identify the forms

Form Number	Form Name
Schedule A (Form 1040)	Itemized Deductions
Form 1040	U.S. Individual Income Tax Return
Schedule C (Form 1040)	Profit or Loss From Business
Schedule EIC (Form 1040A or 1040)	Earned Income Credit
Schedule F (Form 1040)	Profit or Loss From Farming
Form 8888	Allocation of Refund (Including Savings Bond Purchases)
Form W-2	Wage and Tax Statement
Form 1098	Mortgage Interest Statement
Form 1099G	Certain Government Payments
Form 1099MISC	Miscellaneous Income
Form 1041	U.S. Income Tax Return for Estates and Trusts
Form 1120	U.S. Corporation Income Tax Return
Form 1120S	U.S. Income Tax Return for an S Corporation
Form 1065	U.S. Return of Partnership Income
Form 943	Employer's Annual Federal Tax Return for Agricultural Employees
Form 941	Employer's Quarterly Federal Tax Return
Form 940	Employer's Annual Federal Unemployment (FUTA) Tax Return
Form 720	Quarterly Federal Excise Tax Return
Form W-7	Application for IRS Taxpayer Identification Number
IRMF 1098	Mortgage Interest Statement
IRMF 1099	MISC Miscellaneous Income
IRMF W2	Wage & Tax Statement

11f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

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

17a. If yes, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If 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.

19. 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.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	Yes	Read and Write	High

21a. How is access to SBU/PII determined and by whom? Access to the Lead and Case Analytics (LCA) analytic service is requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 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 also performed through the OL5081.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If yes, what date was it completed? 07/10/2017

23.1 Describe in detail the system s audit trail. Accountability, Audit, and Risk Management (AR) This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk. AR-1: Governance and Privacy Program Information System Implementation Status: In Place Inheritance: Fully Inherited (Privacy) NIST SP 800-53 Control: The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures [annually (IRM Exhibit 10.8.1-1 2.1)]. NIST SP 800-53 Control Enhancements: None. IRS Implementation of Control: The privacy controls are under the purview of PGLD office and are covered under their Privacy program. Refer to PGLD for specific details regarding the implementation of this control. AR-2: Privacy Impact and Risk Assessment Implementation Status for LCA: In Place Inheritance: Partially Inherited (Privacy) NIST SP 800-53 Control: The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. NIST SP 800-53 Control Enhancements: None. IRS Implementation of Control: The privacy controls are under the purview of PGLD office and are covered under their Privacy program. Refer to PGLD for specific details regarding the implementation of this control. In accordance with Section 208 of the E-Government Act of 2002,

OMB memorandums, and IRS policy, IRS conducts PCLIAs of electronic information systems that collect and maintain PII and make them publicly available by posting them on IRS.gov; therefore, protecting taxpayer and employee privacy rights. A PCLIA for this system is completed by the system owner or system owner's designee and submitted via the Privacy Impact Assessment Management System (PIAMS) to the Privacy, Governmental Liaison and Disclosure (PGLD) for review and approval. PGLD reviews the PCLIA for any privacy risks and documents their observations in a PCLIA Memo. The PCLIA considers the effects of its actions on the privacy of individuals and ensures that appropriate legal and technical safeguards are implemented. Privacy Monitoring and Auditing: Information System Implementation Status: In Place Inheritance: Fully Inherited (Privacy) NIST SP 800-53 Control: The organization monitors and audits privacy controls and internal privacy policy [at a minimum annually (IRM Exhibit 10.8.1-1 2.4)] to ensure effective implementation. NIST SP 800-53 Control Enhancements: None.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If yes, is the test plan in process or completed: Completed

24.3 If completed or in process**,** 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

24b.1. If completed, 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.)

24b.2. If completed, were all the Privacy Requirements successfully tested? Yes

24.2 If completed, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	Under 50,000
26b. Contractors:	Under 5,000
26c. Members of the Public:	More than 1,000,000
26d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report