Date of Approval: **June 15, 2020**

PIA ID Number: **4749**

SYSTEM DESCRIPTION

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

Investigative Data Examination Application, IDEA

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?

Investigative Data Examination Application, IDEA, 3133, MS4b

What is the approval date of the most recent PCLIA?

2/9/2018

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

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.

Criminal Investigation Governance Board (CI GB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

System Deployment/Milestone 5

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 Investigative Data Examination Application (IDEA) project has a massive amount of heterogeneous data pertinent to financial investigations involving income tax fraud, money laundering and other illegal activities. PII including Social Security Numbers (SSN) are used to associate individuals and entities with financial transactions and as a form of identification. Taxpayer Identification Numbers (TIN) represent taxpayer identification numbers which are composed of social security numbers, entity identification numbers (businesses) and Individual Taxpayer Identification Numbers (ITIN') - assigned to individuals who do not have a social security number. PII is fundamental to data analytics and the identification of association and relationships in the investigation of criminal activity.

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)

The IDEA system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from the Internal Revenue Code (IRC) 6109, which requires an individual taxpayer to include their SSNs on their income tax returns.

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 (OMB Circular A-130) requires that Federal agencies develop a mitigation or elimination strategy for systems the use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record (ex. Taxpayer's Account).

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:

Protection Personal Identification Numbers (IP PIN)

Internet Protocol Address (IP Address)

Criminal History

Certificate or License Numbers

Passport Number

Alien Number

Financial Account Numbers

Tax Account Information

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

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

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

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.

Each data item in the repository will be used for investigations and analysis by the IDEA system. Data available (all from the CI Data Warehouse) to the IDEA repository will be used for both reactive and proactive queries. Reactive queries are a result of specific, targeted investigations, and proactive queries are a result of pattern matching to generate leads. Data available to the repository will enable users to detect suspicious financial transactions that may indicative of money laundering; financial fraudulent schemes; terrorism financing and other financial crimes.

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

The data IDEA receives from the IRS (through the CI Data Warehouse) will be considered as accurate; timely and complete. The data is received "as-is" and deemed accurate. It is assumed that the originating source validates the data for completeness. It is deemed timely in that the most current transactions are received. IDEA will not have the criteria to perform any further verification. Query results will be used for the purpose of generating leads only. Any investigative process that results from these leads will use the corresponding data from the originating systems as the system of record.

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 34.037 Audit Trail and Security Records

IRS 46.050 Automated Information Analysis System

IRS 42.031 Anti-Money Laundering/Bank Secrecy Act and Form 8300

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: Criminal Investigation Management Information System (CIMIS)
Current PCLIA: Yes
Approval Date: 5/9/2019
SA&A: Yes
ATO/IATO Date: 6/20/2019

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: Financial Crimes Enforcement Network (FinCEN)
Transmission Method: Bulk Download to CI Data Warehouse
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: 1040 Form Name: US Individual Income Tax Return

Form Number: 8300 Form Name: Report of Cash Payments over $10,000 in a trade or business

Form Number: 1042-S Form Name: Foreign Person's U.S. Source Income Subject to Withholding

Form Number: SS-4 Form Name: Application for Employer Identification Number

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

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

Form Number: 1098-C Form Name: Contributions of Motor Vehicles, Boats, and Airplanes (Info Copy Only)

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.?

Yes

Briefly explain how the system uses the referenced technology.

The IDEA system is available only within the CI Domain and can be used a Web Application (Intranet via CI issues Computer) or Mobile Application (Intranet (via Derived Credentials on a Corporate Owned Mobile Device) and secure Mobile platform).

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?

Notice is provided to the Taxpayer on the various Forms listed under #11e upon completion and submission. All other information gathered by FinCEN may or may not have received notice as many of the documents are created and filed by Financial institutions as a result of alleged suspicious activity with financial transactions subject to the Bank Secrecy Act (BSA).

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

No

Why not?

The IDEA application does not gather information directly from the individual and the data used in IDEA is a copy of the official record from the source gathering entity or agency.

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

Note: The IDEA application is NOT the system of record for the taxpayer information, therefore correction and redress remain part of the system(s) of record responsibility. The IDEA application does receive corrected and redress data from third party data (ex. FinCEN) [when made available].

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 Contractor Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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

The use of OL-5081, soon to be SailPoint - is a process internal to the Treasury/IRS to manage access to internal application. For IDEA the end-user must have a business need approved by the immediate manager to be granted access to the application.

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.

IDEA is non-recordkeeping. It is not the official repository for any data or documents, rather IDEA is a platform that provides special agents and investigative support staff with a network infrastructure to better perform their jobs. Records created and/or maintained in recordkeeping systems hosted/enlisted by IDEA will be scheduled in the context of those source systems, and records disposition requirements will be documented in the Internal Revenue Service Records Control Schedules (IRM 1.15.8-64, as applicable).

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

6/18/2020

Describe the system's audit trail.

The IDEA application audit model protects privacy and civil liberties by providing data transparency, immutable audit trails and fine-grained server level security controls. Audit trails include information about each time the data is searched and viewed - including by whom and the date & time of the activity. IDEA does not allow the end-user to modify the data. IDEA logs all basic user actions at the system level, including logons, logouts, password changes, searches and record display.

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)?

A summary of results is maintained in a SharePoint repository with permissions restricted to protect both the team and Business Owner.

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?

An Annual Security Control Assessment (ASCA) was finalized for the IDEA application on 5/20/2020. The ASCA is a Continuous Monitoring assessment that ensures all security controls remain in place to properly safeguard PII within the IDEA application.

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: 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?

Yes

Provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

Implementing the 9/11 Commission Recommendations Act of 2017, Public Law 110-53, Section 804.

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

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

The system will provide location information such as a home or business address (sometimes an Internet Protocol (IP) Address) in an effort to locate individuals that are under investigation.

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