Date of Approval: **May 09, 2019**

PIA ID Number: **4060**

SYSTEM DESCRIPTION

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

Criminal Investigation Management Information System, CIMIS

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?

CIMIS Privacy Impact Assessment # 1707

What is the approval date of the most recent PCLIA?

5/27/2016

Changes that occurred to require this update:

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.

Criminal Investigation Governance Board (CIGB)

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 Criminal Investigation Management Information System (CIMIS) consists of two applications: CIMIS and Asset Forfeiture and Retrieval System (AFTRAK). CIMIS is a management tool for tracking the status and progress of Internal Revenue Service (IRS) Criminal Investigations (CI), time expended by employees, employee information, and investigative equipment. AFTRAK is used to manage and track status, inventory and disposition of assets seized and forfeited in the course of CI investigations.

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

Law enforcement and intelligence purposes

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

As federal law enforcement, we are authorized to obtain and use Social Security Numbers (SSNs) for the subjects of our criminal investigations.

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. The CIMIS system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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

Standard Employee Identifier (SEID)

Vehicle Identifiers

Passport Number

Alien Number

Financial Account Numbers

Employment Information

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 (SBUList)

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.

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?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Taxpayer data (Federal Tax Information [FTI])

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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

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.

CIMIS is a management information system central to CI operations. CIMIS tracks and delivers accurate real-time information used for critical oversight of all CI investigations and enforcement actions. Names, addresses, and phone numbers are captured for individuals and entities associated with ongoing criminal investigations. CIMIS data is used to determine future priorities, project staffing, and to account for investigative equipment. Much of the information tracked is required by congressional mandate, Treasury Regulations, Office of Management and Budget (OMB) requirements, and IRS Directives. CIMIS is relied upon heavily for preparing congressional testimony and to ensure CI is successful in achieving IRS' strategic enforcement goals. The use of SSN's: Like the other business operating divisions in IRS, CI uniquely identifies and tracks individuals and businesses under criminal investigation by their Taxpayer Identification Numbers (TINs) in CIMIS. CIMIS collects SSN's on employees because it is often times the only valid way to uniquely identify former employees and employees whose marital status and name have changed.

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

Different levels of CI Management are responsible for reviewing data entries in CIMIS. Periodic reviews and inventories are conducted specifically to measure the accuracy, timeliness and completeness of data entered into CIMIS. In addition, CI Management conducts complete reviews of the inventory within CIMIS once every three years to ensure accuracy. CIMIS does not receive data from other systems. However, for data entered into the system, validity checks within the application are utilized to verify accuracy and completeness.

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

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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: Integrated Data Retrieval System

Current PCLIA: Yes

Approval Date: 10/1/2018

SA&A: Yes

ATO/IATO Date: 10/14/2018

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: Department of Justice

Transmission Method: Received email data file and manual upload to system.

ISA/MOU: Yes

Name: Financial Crimes Enforcement Network (FinCen)

Transmission Method: Received data file and manual upload into system.

ISA/MOU: Yes

Name: United States Postal Inspection Services (USPIS)

Transmission Method: Authorized mail covers

ISA/MOU: No

Name: Department of Homeland SecurIty Customs Border Patrol (SEACATS)

Transmission Method: Received email data files and manual upload to system.

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 Form

Form Number: 1120 Form Name: US Corporation Income Tax Form

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: Dept. of Justice Criminal Tax Division

Transmission Method: Data extract/Email encrypted file

ISA/MOU Yes

Organization Name: Dept. of Justice (FUSION CENTER)

Transmission Method: Data extract/Email encrypted file

ISA/MOU Yes

Organization Name: Dept. of Treasury (FinCEN)

Transmission Method: Data extract/Email encrypted file

ISA/MOU No

Organization Name: Dept. of Treasury (TEOAF)

Transmission Method: Report/Email encrypted file

ISA/MOU Yes

Identify the authority

CIMIS information is shared with our Federal Law enforcement partner agencies on an as-needed basis and solely within the context of investigating Title 26 and Title 18/31 criminal violations and performing seizure and forfeiture activities pursuant to those criminal investigations. Authority to share information is expressly agreed to within each Memorandum of Understanding (MOU).

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

IRS 46.002 - Criminal Investigation Management Information System and Case Files

For what purpose?

Access is needed for tax administration.

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?

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.

Per criminal investigative procedure, potential targets of a criminal investigation are typically not notified that they are under suspicion for committing criminal offenses until such time as they government is ready to prosecute the offender(s).

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

No

Why not?

Per criminal investigative procedure, potential targets of a criminal investigation are typically not notified that they are under suspicion for committing criminal offenses until such time as the government is ready to prosecute the offender(s). Therefore, there would be no opportunity for providing or declining consent.

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

CIMIS stores information on criminal investigations that are placed in our judicial system that adheres strictly to the concept of due process. As applicable, CIMIS data is subject to Freedom of Information Act (FOIA) requests.

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: Read Only

IRS Contractor Employees

Contractor Users: Read Write

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

Based on a user's position and the need-to-know, the manager determines access to the data. The manager will request that a user be added. They must fill out Online 5081, Information System User Registration/Change Request to request access to the application. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Online 5081.

RECORDS SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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 CIMIS system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained 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) 30, Item 50 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)?

In-process

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

5/23/2019

Describe the system's audit trail.

A complete audit trail of the use of the system is captured and includes every login, logoff, file access and database query. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user. CIMIS is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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)?

MIS SharePoint Process Access Library (PAL) website

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?

CIMIS is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

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: 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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes