Date of Approval: **July 29, 2022**

PIA ID Number: **6982**

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 # 4060

What is the approval date of the most recent PCLIA?

5/9/2019

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 and AFTRAK share the same database. Roles and permissions for both applications are managed in CIMIS. 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 tracks assets seized by CI agents during investigations, reports on their status while in government custody, reports on the disposition of assets and distribution of proceeds from asset sales and other disposal methods for forfeited assets. This system supports the IRS CI Asset Forfeiture Program which conducts asset seizure and forfeiture activities in conjunction with criminal investigations and manages asset inventories and the distribution of proceeds under the auspices of the Treasury Executive Office of Asset Forfeiture (TEOAF). IRS CI agents seize assets under Titles 18 (general federal code violations), 21 (food and drug federal code violations), 26 (internal revenue code violations), and 31 (money and finance code violations) of the United States Code (USC).

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)

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)
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers
Employment Information
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.

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 SSNs 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. The AFTRAK system supports the IRS CI Asset Forfeiture Program which conducts asset seizure and forfeiture activities in conjunction with criminal investigations and manages asset inventories and the distribution of proceeds under the auspices of the Treasury Executive Office of Asset Forfeiture (TEOAF). Names, addresses, phone numbers, aliases, and email addresses of individuals who have been identified as having an interest in an asset is captured. AFTRAK also captures the names of agents from other agencies who have requested a share in the proceeds of an asset that their agency helped the IRS seize and forfeit. Depending on the type of asset seized, the asset description captured in AFTRAK may contain identifying information such as bank account numbers, vehicle identification numbers, serial numbers, and license plate numbers.

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. Validity checks within the application are utilized to verify accuracy and completeness of CIMIS data. Similarly, periodic reviews and inventories are done in AFTRAK to ensure accuracy, timeliness, and completeness of data entered. AFTRAK users also run reconciliation reports periodically to reconcile AFTRAK data with data provided by other agencies (e.g., the SEACATS data provided by the Department of Homeland Security Customs Border Patrol).

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:

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: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/1/2021

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: Department of Homeland Security Customs Border Patrol (SEACATS)
Transmission Method: Received email data files and manual upload to system.
ISA/MOU: Yes

Name: United States Postal Inspection Services (USPIS)
Transmission Method: Authorized mail covers
ISA/MOU: No

Does the system receive SBU/PII from State or local agency (-ies)?

Yes

For each state and local 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: Information from state or local agencies could be received externally and used to generate investigations. No ISA or MOU is in place.
Transmission Method: Multiple (digital, phone, etc.)
ISA/MOU: No

Does the system receive SBU/PII from other sources?

Yes

Identify the source 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: General Public
Transmission Method: Receive information from the general public via emails, phone calls, walk-ins, etc.
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1099
Form Name: All Types of Statements for Recipients

Form Number: 943A
Form Name: Agricultural Employer's Record of Federal Income Liability

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

Form Number: 550EZ
Form Name: Annual Return of One-Participant Pension Benefit Plan

Form Number: 5500
Form Name: Annual Return/Report of Employee Benefit Plan (100 or more participants)

Form Number: 5500C
Form Name: Annual Return/Report of Employee Benefit Plan (with fewer than 100 participants, none of whom is an

Form Number: 1042
Form Name: Annual Withholding Tax Return for US Source Income of Foreign Persons

Form Number: 4461
Form Name: Application for Approval of Master or Prototype Defined Contribution Plan

Form Number: 5306
Form Name: Application for Approval of Prototype Individual Retirement Account

Form Number: 5303
Form Name: Application for Determination for Collectively Bargained Plan

Form Number: 5300
Form Name: Application for Determination for Defined Benefit Plan

Form Number: 5301
Form Name: Application for Determination for Defined Contribution Plan

Form Number: 5309
Form Name: Application for Determination of Employee Stock Ownership Plan (ESOP)

Form Number: 1045
Form Name: Application for Tentative Refund

Form Number: 3672
Form Name: Approval of Master or Prototype Plan for Self-Employed Individuals

Form Number: 433-B
Form Name: Collection Information Statement for Business

Form Number: 433-A
Form Name: Collection Information Statement for Individuals

Form Number: 8278
Form Name: Computation and Assessment of Miscellaneous Penalties

Form Number: W-4
Form Name: Employee's Withholding Allowance Certificate

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

Form Number: CT-1
Form Name: Employer's Annual Railroad Retirement and Unemployment Return

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

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

Form Number: 942
Form Name: Employer's Quarterly Federal Tax Return for Household Employees

Form Number: 1040ES
Form Name: Estimated Tax for Individuals

Form Number: 1023
Form Name: Form 1023 is used to apply for recognition as a tax exempt organization under section 501 (c)(3) of

Form Number: 2290
Form Name: Heavy Vehicle Use Tax Return

Form Number: 1040EZ
Form Name: Income Tax Return for Single and Joint Filers With No Dependents

Form Number: 2137
Form Name: Monthly Tax Return-Manufacturers of Cigarette Papers and Tubes

Form Number: 5734
Form Name: Non-Master File Assessment Voucher

Form Number: 656
Form Name: Offer in Compromise

Form Number: 2617
Form Name: Prepayment Return-Tobacco Products Taxes

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

Form Number: 1066
Form Name: Real Estate Mortgage Investment Conduit Income Tax Return

Form Number: 5500R
Form Name: Registration Statement of Employee Benefit Plans

Form Number: 2438
Form Name: Regulated Investment Co.-Undistributed Capital Gains Tax Return

Form Number: 2749
Form Name: Request for Trust Fund Recovery Penalty Assessment

Form Number: 5329
Form Name: Return for Individual Retirement Arrangement Taxes

Form Number: 4720
Form Name: Return of Certain Excise Taxes on Charities and Other persons Under Chap. 41 and 42 of the IRC

Form Number: 5330
Form Name: Return of Initial Excise Taxes Related to Employee Benefit Plans

Form Number: 990
Form Name: Return of Organization Exempt from Income Tax Return

Form Number: 11C
Form Name: Special Tax Return and Application for Registry-Wagering

Form Number: 5227
Form Name: Split-Interest Trust Information Return

Form Number: 730
Form Name: Tax on Wagering

Form Number: W-3
Form Name: Transmittal of Income and Tax Statements

Form Number: 1040A
Form Name: U.S Individual Income Tax Return (Short form)

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

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

Form Number: 1041
Form Name: U.S. Fiduciary Income Tax Return (for Estates and Trusts)

Form Number: 8453
Form Name: U.S. Individual Income Tax Declaration for Electronic Filing

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

Form Number: 957
Form Name: U.S. Information Return by an Officer, Director, or U.S. shareholder with Respect to a Foreign Perso

Form Number: 1040NR
Form Name: U.S. Nonresident Alien Income Tax

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

Form Number: 1040PR
Form Name: U.S. Self-Employment Tax Return-Puerto Rico

Form Number: 1040SS
Form Name: U.S. Self-Employment Tax Return-Virgin Islands, Guam, American Samoa

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

Form Number: 706
Form Name: United States Estate Tax Return

Form Number: 709
Form Name: United States Gift Tax Return

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 fil
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

Contractor System Administrators: Administrator

Contractor Developers: Administrator

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 user must submit a request within the Business Entitlement Access Request System (BEARS). The manager will then review and approve the request. 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 BEARS. Once the BEARS access request is approved, a CIMIS user administrator will go in and assign the appropriate role(s) and scope for each role to the user.

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 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)?

Yes

What date was it completed?

6/9/2022

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)?

Management Information System (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