Date of Approval: 11/20/2024
Questionnaire Number: 1410

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Criminal Investigation Management Information System, CIMIS

Acronym:

CIMIS

Business Unit

Criminal Investigation

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

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).

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

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 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.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Agency Sensitive Information

Alien Registration Number

Centralized Authorization File (CAF)

Driver's License Number

Education Information

Email Address

Employment Information

Family Members

Financial Account Number

Individual Taxpayer Identification Number (ITIN)

Internet Protocol Address (IP Address)

Name

Official Use Only (OUO) or Limited Office Use (LOU)

Passport Number

Professional License Number

Protected Information

Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)

Tax ID Number

Telephone Numbers

Vehicle Identification Number (VIN)

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

Information by CI for certain money laundering cases - 18 USC

PII about individuals for Bank Secrecy Act compliance - 31 USC

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

PII for personnel administration - 5 USC

SSN for personnel administration IRS employees - 5 USC and Executive Order 9397

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

System

1.35 Is there a data dictionary for this system?

Yes

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

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).
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).

1.4 Is this a new system?

No

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.6 What is the PCLIA number?

6982

1.7 What are the changes and why?

Addition of IP Address and Splunk SORN.

1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

210266 (CIMIS), 210054 (AFTRAK)

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Execution

1.95 If this system has a parent system, what is the PCLIA Number of the parent system?

No

2.1 If this system discloses any PII to any third party outside the IRS, 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. Enter "Yes" or "No". If Exempt, type "Exempt".

Yes

2.2 Please provide the full name of and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Criminal Investigation Governance Board (CIGB

3.1 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960?

No

3.3 Does this system use cloud computing?

No

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

Not a public application

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Contractor Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

Yes

4.3 What PII/SBU data does the subcontractor have access to?

Name Mailing address Phone Numbers E-mail Address Date of Birth Standard Employee Identifier (SEID) Internet Protocol Address (IP Address) Certificate or License Numbers Vehicle Identifiers Passport Number Alien Number Financial Account Numbers Employment Information Tax Account Information Centralized Authorization File (CAF)

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

Employee Users - Read/Write Employee Managers - Read/Write Employee System Administrators - Read-Only Contractor Users - Read/Write - Background Investigation Required Contractor System Administrators - Administrator - Background Investigation Required Contractor Developers - Read/Write - Background Investigation Required

4.51 How many records in the system are attributable to IRS Employees? Enter “Under 50,000”, “50,000 to 100,000”, “More than 100,000” or “Not Applicable”.

Under 50,000

4.52 How many records in the system are attributable to contractors? Enter “Under 5,000, “5,000 to 10,000”, “More than 10,000” or “Not Applicable”.

Under 5,000

4.53 How many records in the system are attributable to members of the public? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not applicable”.

More than 10,000

4.54 If records are attributable to a category not mentioned above in 4.51 through 4.53, please identify the category and the number of corresponding records to the nearest 10,000. If none, enter "Not Applicable".

Not Applicable

4.6 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.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

There are currently no Privacy, Civil Liberties or Security Risks identified with the application.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

Local Agencies

Agency Name

Information from state or local agencies could be received externally and generate investigations

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Other

Other Transfer Method

Multiple (digital, phone, etc.)

Interface Type

Other Federal Agencies

Agency Name

Department of Justice

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Secure email/Zixmail

Interface Type

Other Federal Agencies

Agency Name

Financial Crimes Enforcement Network (FinCEN)

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Secure email/Zixmail

Interface Type

Other Federal Agencies

Agency Name

United States Postal Inspection Services (USPIS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Mail

Interface Type

Other Federal Agencies

Agency Name

Department of Homeland Security Customs Border Patrol (SEACATS)

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Secure email/Zixmail

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 46.002 - Criminal Investigation Management Information System and Case Files

Describe the IRS use and relevance of this SORN.

SORN for the system

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

CIMIS contains audit data that is ingested by SPLUNK.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Criminal Investigation - 30

What is the GRS/RCS Item Number?

77

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

CIMIS is the 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. CIMIS data is used to determine future priorities, project staffing, and to account for investigative equipment. CIMIS is a database that tracks data in six main areas: 1. Investigations, 2. Monthly Activity Reports (aka Form 5043), 3. Equipment, 4. Personnel, 5. Audit Trail Information. 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.
CIMIS is also the central web platform with which the following systems are currently integrated: •AFTRAK (CI's Asset Forfeiture tracking system)

What is the disposition schedule?

AUTHORIZED DISPOSITION Cut off 2 years after the following applicable conditions have been met: •status of investigation is referred to civil or no civil action required; •all asset forfeiture

activities are completed; •conditions of probation have been met. Delete 8 years after cutoff. 2. Monthly Activity Reports (aka Form 5043) Data. Time charged to investigative and non-investigative activities by CI employees. (Job No. DAA-0058-2019-00030002) AUTHORIZED DISPOSITION Cut off 2 years after the end of the calendar year in which they were recorded. Delete 8 years after cutoff.3. Equipment Data. Assignment and inventory information for sensitive law enforcement equipment (e.g. weapons, badges, motor vehicles, etc.). (Job No. DAA-0058-2019-0003-0003) AUTHORIZED DISPOSITION Cut off 2 years after final disposal of equipment record. Delete 8 years after cutoff. 4. Personnel Data. Employee and non-CI employee identifying information to create assignments of investigations and equipment; manage user roles and permissions throughout CIMIS; and/or provide adequate audit trail information. (Job No. DAAÂ 0058-2019-0003-0004) AUTHORIZED DISPOSITION Cut off 2 years after personnel profile record has been terminated. Delete 8 years after cutoff, or when the personnel record no longer has any association to any other existing CIMIS data records (whichever is later). 5. Public Information Office Outreach Data. Data on the organizations to which CI employees give presentations regarding the CI mission and program areas.
(Job No. DAA-0058-2019-0003-0005) AUTHORIZED DISPOSITION Cut off 3 years after event occurs. Delete 4 years after cutoff. Note: As of Dec 2017, no longer accumulated. 6. Audit Trail Data. This is a distinct set of data that is captured in the database expressly for audit trail purposes. (Job No. DAA-0058-2019-0003-0006) AUTHORIZED DISPOSITION Delete 7 years after date of capture. Disposition was too long program would not accept length over 2000.

Data Locations

What type of site is this?

System

What is the name of the System?

Criminal Investigation Management Information System (CIMIS & AFTRAK)

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

https://cimis

Please provide a brief description of the System.

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).

What are the incoming connections to this System?

Ingest minimal Asset Forfeiture data from AFTRAK Web Services

What are the outgoing connections from this System?

CIMIS provides case (investigation, identity, warrant), organization, user/role, general reference (state, country, CI Program, Judicial District), and personnel data to AFTRAK CIMIS also provides investigation data to International Database (IDB) CIMIS also provides audit data (Windows Application Event Log, Internet Information Services Log, SQL Trace Files) to Splunk.