Criminal Investigation Management Information System (CIMIS) Release 2.9 Planned Maintenance – Milestone 4b – Privacy Impact Assessment

PIA Approval Date – Oct. 25, 2011

System Overview

The Criminal Investigation Management Information System (CIMIS) is a management tool for tracking the status and progress of Internal Revenue Service (IRS) Criminal Investigation (CI) investigations, time expended by CI employees, employee information, and IRS CI investigative equipment. CIMIS is the vehicle that collects, compiles, and delivers information on investigative activities and legal actions to authorized users within CI. Data contained in CIMIS is also used to respond to congressional mandates, Treasury regulations, Office of Management and Budget (OMB) requirements, and IRS directives. CIMIS is the official source of information used by IRS CI when preparing statistical information for congressional testimony and for releasing statistical information on prosecutions resulting from CI investigations to the media. Capabilities include direct data entry from the field, real time query, and report features. Data from this application is also exported to other applications. These include the Investigative Data Analytics (IDA), Evidence Management and Collaboration Systems (EMACS), and International Operations (IO) as well as several other systems and/or agencies external to the IRS, including the Treasury Enforcement Communication System (TECS) and the FUSION Center.

The CIMIS application is integrated with the Asset Forfeiture Tracking and Retrieval (AFTRAK) and PIOneer (PIO) applications. AFTRAK tracks assets seized by CI agents during investigations and their status while in government custody, and tracks and 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 that 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). The web-based PIOneer application's purpose is to associate and track media and investigation information for Criminal Investigation's (CI) Public Information Officers (PIO). The PIOneer Application allows the PIOs nation–wide and the CI Headquarters (HQ) staff to collect, monitors, and report upon incoming and outgoing media correspondences, related investigations and associated legal actions. This tool enables the PIO to be more effective in their communication and outreach to the media and public outlets with the ability to search and store related media documents directly with the associated investigation.

Systems of Records Notice (SORN):

- IRS 46.002--Criminal Investigation Management Information System
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

CIMIS:

A. Taxpayer – Includes data related to the identity of the individual, the tax forms and periods, an estimated criminal tax deficiency, terms of probation involving taxes, and other information regarding potential criminal tax and other financial investigations.
   - Name
   - Doing Business As (DBA)

- Alias, Identity Type
- Affiliation to Subject
- Taxpayer Identification Number (TIN)
- Other Identifying Numbers (driver's license, passport, etc.)
- Address
- Date of Birth
- Gender
- Type of Tax Forms
- Preparer Name
- DOJ Attorney Name/Position
- Location of Monitoring Devices

B. CI Employee:

1. Compared to investigative data, employee data is stored in separate business tables, tracked in separate log tables, and access granted based on separate user roles.
    - Name
    - SSN (employee SSNs are partially masked in the majority of the screens and reports, with the ultimate goal being the elimination of employee SSNs from the CIMIS database altogether)
    - Identification Number (SEID)
    - Date of Birth
    - Retirement Plan and 6C Date
    - Service Computation Date
    - Award/Type, Type/Date of Background Investigation
    - Security Clearance, Skills
    - Education/Degree/Graduation
    - Position
    - Management Assignments and Training
    - Time Reporting Data
    - Phone number

2. Non–CI Employee: Non–CI employee data is limited to name, title and organization within specific investigative data, e.g., a requesting or cooperating revenue agent. The employee can be another IRS employee.
    - Name
    - SSN – non–employee SSNs are partially masked in the majority of the screens and reports, with the ultimate goal being the elimination of employee SSNs from the CIMIS database altogether)
    - Address
    - Phone Information
    - CI Affiliation

C. Audit Trail:

- Date/Time Stamp (The Date/Time of when the audit record was created)
- Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID)
- Event Type (The Event Type field is used to track the type of event that is executed such as create, update, or delete)
- Origin of Request (The origin of where the request was made, such as the Terminal ID)
- Name of Object (The name of the object that was introduced, accessed, or deleted)
- User Identity (The identity of the user who performed the action)

- User Role (The role of the user at the time the action was performed)

D. Other – Inventory and assignment of equipment and vehicle expense and mileage information. Strictly speaking, the below data does not contain privacy information; however, equipment inventory is tied to an employee within CIMIS, and as a result could be used to ultimately identify an individual.

- Equipment ID Number
- Order Information (date, intended organization, etc.)
- Acquisition Information (date, amount, etc.)
- Category/Sub-category/Sub–category Class
- Description
- Purpose
- Manufacturer
- Model
- Serial Number
- Vehicle Specific Information (model year, license plate #, initial odometer reading, etc.)
- Vehicle Maintenance Expenses and Mileage Information
- Shipment and Consignment Information
- Assignment and Storage Information
- Disposal Information (dates, disposal, proceeds)

AFTRAK:

A. Taxpayer:

- Name
- Doing Business As (DBA)
- Alias
- Address
-

B. Employee:

- Seizing Agent First and Last name (this information is retrievable from CIMIS but never stored as data elements in AFTRAK)
- Asset Forfeiture Coordinators First and Last Name, Phone Number, and Address

C. Audit Trail:

- Date/Time Stamp (The Date/Time of when the audit record was created)
- Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID)
- Event Type (The Event Type field is used to track the type of event that is executed such as create, update, or delete)
- Origin of Request (The origin of where the request was made, such as the Terminal ID)
- Name of Object (The name of the object that was introduced, accessed, or deleted)
- User Identity (The identity of the user who performed the action)
- User Role (The role of the user at the time the action was performed)

D. Other:

- Information on individuals who have been identified as having an interest in an asset (such as an owner, lien, claim, or petition). This information includes: Name, Address, Phone Numbers, Aliases, Email Address, Attorney Name, Attorney Phone, Attorney Fax, and Attorney Email Address

- Contact Names of agents from other agencies (federal, state, or local) that have requested a share in the proceeds of an asset that their agency helped IRS seize and forfeit
- Names and addresses of Storage Location Vendors
- Asset description may contain identifying information, to include bank account numbers and vehicle identification numbers. This depends on the type of asset seized
- Vehicle Identification Numbers, Serial Numbers, License Plate Numbers, and Account Numbers are also stored

PIOneer:

A. Taxpayer – Identity of the subject of an investigation. Data includes:
   - Name
   - Taxpayer Identification Number (TIN)
   - Date of Birth (DOB)
   - Address
   - Aliases
   - Occupation
   - Industry

B. Employee:
   - Name
   - Post of duty
   - Phone/email contact information for all agents assigned to a case

C. Audit Trail Information (including employee log–in info):
   - The system records all data queries and data changes made, recording the date/time of the access/change and user's network login
   - Web service logs track view page requests to the server, and the server's responses

D. Other (Describe):
   - Data about criminal investigations in progress, including information about the alleged violation, violation type (statute), CI program areas, investigation status, assigned Assistant United States Attorney (AUSA) or Department of Justice (DOJ) attorney name, address, phone, name of the judge, address of courthouse links to documents about investigative actions
   - Number Optional feature: Records of media contacts, including name, title, organization, address, phone/fax/email, contact date, topic of contact
   - Records of outreach activities, including organization name, type, date/time of event, event address, organization contact name, phone, email, fax, date of request, assigned speaker name/title, office, event history, links to documents about the outreach event
   - System Data: SEID or Login ID, machine name, and IP addresses

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

CIMIS:

A. IRS – IDRS (identity and tax return information – see 1.A above) – this data is manually entered into CIMIS.

B. Taxpayer – Identity and tax return information may be provided by the taxpayer or their designated representatives through interviews and document requests (identity and tax return information, see 1.A above)

C. Employee – all employee related information, see 1.B above.

D. Other Federal Agencies – Agency investigative data is generally not reflected in CIMIS; however, some exceptions include:
   - The Department of Justice (DOJ) may provide administrative information (legal opinions/authorizations) and results of judicial proceedings that are reflected in CIMIS as status and/or arrest/fugitive updates
   - Financial Crimes Enforcement Network (FinCEN) may provide taxpayer identity information (see 1.A above)
   - United States Postal Inspection Service (USPIS) may supply mail cover approvals and corresponding dates
   - Any agency may provide or confirm identity information and criminal allegations

E. State and Local Agencies – Agency investigative data is generally not reflected in CIMIS. Any agency may provide or confirm identity information and criminal allegations. (Taxpayer identity information, see 1.A above.)

F. Other third party sources – Informants and other third party source information is generally not reflected in CIMIS. Their names may be listed as associate identities or they may provide additional taxpayer identifying information and criminal allegations. (Taxpayer identity information, see 1.A above). Time reporting data may be uploaded from the Diary application that is part of the CI Standard Applications package residing on the agents' personal workstations.

AFTRAK:

A. IRS – The CIMIS Number is fully integrated with the AFTRAK system. The application pulls in data from the application to reduce redundancy of data.

B. Employee – all employee related information, see 1.B above.

C. Other Federal Agencies – TEOAF provides National Finance Center (NFC) data that is matched with data in AFTRAK. Users view reports showing matched and unmatched data in order to reconcile differences. This information contains no privacy information, and is only an asset number and an amount. In addition, AFTRAK stores data received from DOJ that contains information concerning Reverse Asset Sharing Requests (RASR).

   U.S. Customs Seizure Case and Asset Tracking System (SEACATS) data is provided to AFTRAK via Contract Asset Property Managers. The SEACATS data is matched with data in AFTRAK. Users view reports showing matched and unmatched data in order to reconcile differences. This information contains vendor name and address.

D. Third Party Resources: A Contract Asset Property Manager provides US Customs SEACATS data.

PIO:

A. IRS – PIOneer queries the following information from the Criminal Investigation Management Information System (CIMIS):

- Data about the Subject of the investigation
- Data about criminal investigations
- Data about the Special Agents assigned to the investigation, such as CI Field office location
- PIOneer Application users manually enter data provided by contacts for:
- Records of outreach events
- Records of contact with members of the media or other public information contacts
- Data about attorneys and judges involved in legal actions

3. Is each data item required for the business purpose of the system? Explain.

CIMIS:

- Yes. The data collected is required for CIMIS to track CI investigations, employee data, hours spent on investigations, and equipment inventory.

AFTRAK:

- Yes. Assets must be stored and maintained by the government until asset disposition decisions are made. AFTRAK is the inventory tool for these assets that supports the business purpose of the system.

PIOneer:

- Yes. All data is required for the business purposes and operations of the system. The business purpose of the system is to track legal actions and store publicity information related to criminal investigations. The system also stores data about community outreach events managed by the Public Information Officer as part of his/her official duties.

4. How will each data item be verified for accuracy, timeliness, and completeness?

CIMIS:

- 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.

AFTRAK:

- The Asset Forfeiture Specialist employee category of users is made up of contractors responsible for entry of the data that is then validated by the Asset Forfeiture Coordinator. The business rules built into the application ensure that accuracy and completeness of the data entered. Manual imports of extracts from the following external entities are received: The TEOAF, National Seized Property Contractors (NSPC), and the DOJ. The data that is imported is reconciled against the data that is input through the AFTRAK user interface for accuracy. The imports themselves are used as a mechanism to verify that the data in AFTRAK is accurate.

PIOneer:

- Data provided by CIMIS is verified by CIMIS users and managers. PIOneer connects to CIMIS through a web service to gain access to investigation data in real time. Data entered by PIOneer users is manually reviewed for accuracy, timeliness and completeness throughout the investigation lifecycle.

5. Is there another source for the data? Explain how that source is or is not used.

CIMIS:

- Yes. Employee time records can be accessed via Diary. Diary is a desktop application used by agents to record their time. While CIMIS is the source of record, data is also stored in the desktop application. However, there is no other source of data for the type of information that will be contained in CIMIS.

AFTRAK:

- No. There are no other sources of data beyond what has been mentioned previously in this PIA.

PIOneer:

- No. There are no other sources of data beyond what has been mentioned previously in this PIA.

6. Generally, how will data be retrieved by the user?

CIMIS:

- Data will be retrieved either through the view and edit capability of the application, from preformatted reports, and/or a designed query.

AFTRAK:

- AFTRAK application users can use the Investigation Number, Seizure Number and AFTRAK Number to retrieve data. The investigation number is directly related to the CIMIS investigation. The seizure number is only an identifying number for AFTRAK and not privacy related data. The AFTRAK Number is a unique identifier for the specific assets related to a seizure and does not contain privacy related data. Report users retrieve data based on the data scope. Data scope is National (all data), or regional (data for all field offices in region, or field office (only data within their field office).

PIOneer:

- Authorized users will use a report creation and search function in the PIOneer application to retrieve data, based on access rights and permissions.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

CIMIS:

- Yes. However, employee data is only retrievable by SSN by HQ staff charged with data administration. End users are not able to retrieve employee records by searching on SSN.
- CI Employee data must be maintained per Internal Revenue Manual (IRM) 1.15.30 Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003. Prior to the SEID number being assigned to IRS CI employees, only the SSN was used to provide information on CI employees. The SSN is the only valid number to identify former employees and employees whose marital status has changed, i.e., last name.
- Investigation data can be retrieved by name, TIN and system generated unique identifier.
- Equipment data can be retrieved by assignment name and a system generated unique identifier.

AFTRAK:

- Yes. Employee data may be retrievable by first name or last name. AFTRAK does not store SSN or TIN.

PIOneer:

- Yes. Data can be retrieved using the first or last name of subject (person or business) or first or last name of the agent. Data cannot be retrieved by SSN or TIN.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

CIMIS/AFTRAK/PIOneer – All CI personnel (Users, Managers, System Administrators, Developers, Others) can gain access to the system if approved by management. Access is removed when no longer needed for job duties assigned.

9. How is access to the data by a user determined and by whom?

CIMIS/AFTRAK/PIOneer – The manager based on a user's position and need–to–know determines access to the data. The manager will request that a user be added. They must fill out Form 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 Form 5081.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.

CIMIS:

Yes. CIMIS does not receive any data from other IRS systems; however, the following systems receive limited data from CIMIS:

- Investigative Data Analytics (IDA):
    - Taxpayer Name
    - Alias
    - Address
    - Date of birth
    - Gender
    - Preparer Name

AFTRAK:

Yes. CIMIS is directly integrated with the AFTRAK application. CIMIS provides AFTRAK with investigation and warrant information for which CIMIS is the system of record. The following system sends limited data to AFTRAK:

- Integrated Financial System (IFS)

PIOneer:

PIOneer retrieves the following information from the CIMIS:

- Data about the Subject of the investigation
- Data about criminal investigations
- Data about the Special Agents assigned to the investigation, such as CI Field office location

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Criminal Investigation Management Information System/Asset Forfeiture Tracking and Retrieval (AFTRAK) CIMIS/AFTRAK:

- Security Assessment & Authorization (SA&A) – April 8, 2010
- Privacy Impact Assessment (PIA) – October 25, 2011

PIOneer

- Security Assessment & Authorization (SA&A) – June 19, 2009
- Privacy Impact Assessment (PIA) – February 4, 2009

Investigative Data Analytics (IDA)

- Security Assessment & Authorization (SA&A) – March 16, 2011
- Privacy Impact Assessment (PIA) – July 14, 2011

Integrated Financial System (IFS)

- Security Assessment & Authorization (SA&A) – May 26, 2010
- Privacy Impact Assessment (PIA) – June 3, 2008

Criminal Investigation – 1 (CI–1)

- Security Assessment & Authorization (SA&A) – June 10, 2011
- Privacy Impact Assessment (PIA) – May 25, 2011

12. Will other agencies provide, receive, or share data in any form with this system?

CIMIS:
Yes. CIMIS does not receive any data from other agencies; however, CIMIS may provide the following information:

- Audit logon information to the GAO and/or TIGTA pursuant to an investigation and/or their oversight function;
- Investigation information to the FinCEN, TIGTA, TECS, and the FUSION Center;
- Equipment information to the Department of Treasury, GSA, and the GAO; and
- A data extract to the FinCEN, the administrator of the Bank Secrecy Act (BSA).

AFTRAK:
Yes. TEOAF receives Title 18, 21, and 31 monthly and quarterly paper reports, and various ad hoc reports from AFTRAK via manual transmission. A formal data sharing agreement exists with TEOAF. AFTRAK will receive an extract from the DOJ containing information pertaining to the state of the Reverse Asset Sharing Report (RASR).

PIOneer:
No other agencies will provide, receive, or share data in any form with the system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

CIMIS/AFTRAK/PIOneer:
Criminal Investigation is currently awaiting NARA approval for its proposed records retention process whereby, at the end of the specified retention period, all personally identifiable information is

eliminated in CIMIS and AFTRAK records. Once approved, this process will be developed and implemented as soon as possible within the constraints of available funding and resources.

14. Will this system use technology in a new way?

CIMIS/AFTRAK/PIOneer:
No. CIMIS will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.

CIMIS:

- Yes. CIMIS is the vehicle that collects, compiles, and delivers information on investigative activities to target an individual or group for tax law violations.

AFTRAK:

- No. AFTRAK will not be used to identify or locate individuals or groups.

PIOneer:

- Yes. The business purpose of this information is to enable the Public Information Officer to accurately respond to inquiries from the media, and to contact journalists or organizations who have made inquiries. The location of legal actions related to an investigation determines the location of media outlets that may contain publicity about the investigation. Tracking the publicity is a business purpose of PIOneer.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.

CIMIS:

- Yes. Monitoring the case lifecycle against an individual, organization, business, etc is the business purpose of the system.

AFTRAK/PIOneer:

- No. The application modules will not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?

CIMIS:

- Yes. CIMIS is the vehicle that collects, compiles, and delivers information on investigative activities to target an individual or group for tax law violations. Therefore, by creating a case against a person who violates tax laws, CIMIS treats him/her differently from those who do not.

AFTRAK/PIOneer:

- No. The application modules will not allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

CIMIS:

- Yes. CIMIS stores information on criminal investigations that are placed in our judicial system that adheres strictly to the concept of due process.

AFTRAK:

- No. AFTRAK is only an inventory tool and does not have the capability to make negative determinations.

PIOneer:

- Not applicable. PIOneer does not make any determinations about affected parties.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?

CIMIS/AFTRAK/PIOneer:

- CIMIS is an intranet web–based system for authorized CI employees. Cookies are not used to track access. Audit logs and trails are used by CIMIS to track CI user access.

View other PIAs on IRS.gov