Criminal Investigation – 1 General Support System (CI–1 GSS) – Privacy Impact Assessment

PIA Approval Date – May 25, 2011

System Overview

The Criminal Investigation – 1 General Support System (CI–1 GSS) is integral in supporting the mission of CI–I as the GSS provides network connectivity to internal CI applications Criminal Investigation Management Information System (CIMIS), Public Information Officer Database (PIOneer), and other IRS applications such as the Integrated Data Retrieval System (IDRS). The CI network provides users with the necessary infrastructure to access e–mail services, file services, print services, and access to management and inventory database systems. The network operates on top of the IRS wide area network (WAN) with CI local area network (LAN) segments isolated behind CI routers for additional layer of security.

Systems of Records Notice (SORN):

- IRS 46.002--Criminal Investigation Management Information System
- IRS 46.009--Centralized Evaluation and Processing of Information Items, Evaluation and Processing of Information, Criminal Investigation Division
- IRS 46.022--Treasury Enforcement Communications System, Criminal Investigation Division
- IRS 46.050--Automated Information Analysis 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:

CI–1 GSS is comprised of network infrastructure, servers and workstations. These workstations and servers function as file servers and store employee work products, which contain the following information types. This work product is not searchable or accessible at the infrastructure level.

A. Taxpayer – CI–1 GSS taxpayer information includes the following:
   - Name
   - Address
   - SSN
   - TIN
   - Birth–date
   - Filing Status
   - Special Agent Reports: These reports include wide–ranging financial information, potential charges, and criminal activity of a taxpayer.
   - Scanned Bank Records from financial institutions.

B. Employee:
   - Standard Employee Identifier (SEID)

C. Audit Trail Information:
   - Servers:
     - Audit Account Logon Events
     - Success and Failures
     - Audit Account Management Success and Failure
     - Audit Directory Server Access (Failures Only)
     - Audit Logon Events (Success and Failure)
     - Audit Object Access (Failure)

- Audit Policy Change (Success and Failures)
- Audit Privileged Use (Failure)
- Audit System Events (Success and Failures)

D. Other – Other information types stored by the GSS include:
   - Employee Investigative Work Product related to Criminal Investigation and Surveillance, Legal Investigation, Substance Control, Judicial Hearings, and Grand Jury.

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

A. IRS – IDRS/Electronic Fraud Detection System (EFDS)/ Account Management System (AMS):
   - Name
   - Address
   - SSN
   - SEID
   - TIN
   - Birth–date
   - Filing Status is manually obtained from tax returns, IDRS, individuals and any other potential IRS applications used for investigative research.

   Employee Information, such as personnel, payroll, and evaluation data. All taxpayer–related information covered by § 6103 of the Internal Revenue Code. Name, Home address, Social Security number, Date of birth, Home telephone number

B. Employee – The CI–1 GSS receives employee SEID for logon purposes.

C. Other Federal Agencies – HR Connect: The CI–1 GSS receives information from HR Connect, which includes information from other Federal Agencies (Federal Bureau of Investigation, Drug Enforcement Administration, Alcohol, Tobacco and Firearms, United States Secret Service, Financial Crimes Center, United States Postal Service Inspectors, Homeland Security) including:
   - Name
   - Address
   - SSN
   - TIN
   - Birth–date
   - Criminal History as investigative information contained in employee work products.

D. State and Local Agencies – State and Local Agencies (State Bureaus of Investigation, Attorney Generals, Local Law Enforcement, State Tax Agencies) provide information to the CI–1 GSS including:
   - Name
   - Address
   - SSN
   - TIN
   - Birth–date
   - Criminal History as Investigative Information.

E. Other Third Party Sources – The CI–1 GSS also receives information from other third party sources, including search warrants and informants including
   - Name
   - Address
   - SSN

- TIN
- Birth–date
- Criminal History as Investigative Information.

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is required for the business purpose of the system. The data items are required to support the mission of Criminal Investigation in investigating criminal tax and financial crimes. The business purpose of the system is to support Criminal Investigation employees in the execution of their duties in support of that mission.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Data items are verified for accuracy, timeliness and completeness as part of a manual process performed by the employees and management in the process of conducting investigations and prosecutions. The CI–1 GSS network is nothing but a repository of information from other systems, so the CI–1 GSS relies on other systems to verify accuracy, timeliness, and completeness of information.

5. Is there another source for the data? Explain how that source is or is not used.
Yes, every federal and state agency is a potential source, and every county and state is a potential source. Therefore, the CI–1 GSS has thousands of sources, so it is not feasible to list every potential source to the CI–1 GSS. Any local, municipality, county, state, or federal information source is a potential information source, as well as privately owned information such as banks.

6. Generally, how will data be retrieved by the user?
Data is retrieved from the user's workstation or the server. Each user must have a CI–1 username and password to use their workstation. In the future, SharePoint will be used as a central repository for all CI–1 GSS case–related data, so that users will be using the SharePoint site instead of individual workstations to pull case data.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
No, none of the data within the CI–1 GSS is retrievable by personal identifier, such as name, SSN, or other unique identifier.

Access to the Data

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

Role: System Administrators,
Permission: Have access to case data stored on local servers. The owning CI employee has access to their own information and share areas based on the CI Active Directory group membership.

Role: Managers,
Permission: Have access to case data stored on local servers. The owning CI employee has access to their own information and share areas based on the CI Active Directory group membership.

Role: Computer Operations Administrator (COA)
Permission: Have access to case data stored on local servers. The owning CI employee has access to their own information and share areas based on the CI Active Directory group membership.

Role: Administrators
Permission: On CI–1 servers, administrators by virtue of the privileges delegated to them, have access to all information in their areas, with the exception of restricted databases. A limited number of administrators at the National Operations Center (NOC) have administrator access to all network resources, with the exception of restricted databases. All administrative access is logged. All administrative duties are performed using a separate administrator account. On CI–1 workstations, administrators do not have access to any encrypted user data unless the data recovery agent is enabled, which requires change control since the account is normally disabled.

9. How is access to the data by a user determined and by whom?
User access is authorized by management through Online 5081 and the 2,700 CI Active Directory groups. Users receive the rules of behavior and employees and management must recertify the employee's need/access annually.

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.
The following IRS systems provide, receive, or share data with CI–1 GSS including:

- Integrated Data Retrieval System (IDRS):
  - Name
  - Address
  - SSN
  - SEID
  - TIN
  - Birth–date
  - Filing Status is manually obtained from tax returns, IDRS, individuals and any other potential IRS applications used for investigative research.

- Electronic Fraud Detection System (EFDS):
  - Name
  - Address
  - SSN
  - SEID
  - TIN
  - Birth–date
  - Filing Status is manually obtained from tax returns, IDRS, individuals and any other potential IRS applications used for investigative research.

- Account Management System (AMS):
  - Name
  - Address
  - SSN
  - SEID
  - TIN
  - Birth–date
  - Filing Status is manually obtained from tax returns, IDRS, individuals and any other potential IRS applications used for investigative research.

- Corporate Authoritative Directory Services (CADS) (Part of Modernization & Information Technology Services (MITS)–17 General Support System (GSS)
  - Global Address List

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

Integrated Data Retrieval System (IDRS)

- Certification & Accreditation (C&A) Authority to Operate (ATO) – March 10, 2009, expires March 10, 2012
- Privacy Impact Assessment (PIA) – November 6, 2008, expires on November 6, 2011

Electronic Fraud Detection System (EFDS)

- Certification & Accreditation (C&A) Authority to Operate (ATO) – June 20, 2008, expires June 20, 2011
- Privacy Impact Assessment (PIA) – October 7, 2008, expires on October 7, 2011

Account Management System (AMS)

- Certification & Accreditation (C&A) Authority to Operate (ATO) – August 3, 2009, expires August 3, 2012
- Privacy Impact Assessment (PIA) – November 10, 2009, expires on November 10, 2012

Corporate Authoritative Directory Services (CADS)

- Certification & Accreditation (C&A) Authority to Operate (ATO) – September 24, 2010, expires September 24, 2013
- Privacy Impact Assessment (PIA) – February 19, 2010, expires on February 19, 2013

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, other agencies will provide, receive, or share data with the CI–1 GSS through a manual process of employees sharing data from their workstation on a specific case, i.e., a printed memorandum. Audit log information may be provided TIGTA pursuant to an investigation and/or their oversight function.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
Employee work products are retired based on the disposition requirements for that type of document. They are retired in a manual, operational process that is not a function of the system. Server backups are retained indefinitely due to support prosecution appeals. User account data is comprised of user login information. When employees leave the service, user accounts are deleted and proper documentation is maintained for 6 years in case it's needed as a result of an internal inquiry. Records control is covered by IRM 1.15.30, Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003, and IRM 1.15.20, Records Control Schedule for Administrative/Organization Support Operational Records, October 19, 2010. The CI–1 GSS is required to hold onto case data for 10 years from the date of the final appeal.

14. Will this system use technology in a new way?
No, the CI–1 GSS does 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.
No, the CI–1 GSS is not used to identify or locate individuals or groups.

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.
No, the CI–1 GSS does not provide the capability to monitor individuals or groups, although they do audit CI employees using the CI–1 workstations and servers.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No, the system does not allow the 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?
No, the CI–1 GSS is not capable of making any determinations on either taxpayers or employers

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No, the CI–1 GSS does not user persistent cookies or other tracking devices to identify web visitors, as only IRS CI users have access to the GSS.

View other PIAs on IRS.gov