Chief Counsel System Domain (CC – 1) – Privacy Impact Assessment

PIA Approval Date – December 15, 2010

System Overview:
The Chief Counsel System Domain referred to as the CC–1 General Support System (GSS) is responsible for providing the network infrastructure for attorneys and support personnel. The applications are both Commercial off–the–shelf (COTS) and in–house developed applications. The CC–1 GSS implements many of its own controls, rather than relying (inheriting) on another GSS or from an Organization Common Control (OCC). The CC–1 GSS includes Windows 2003/2008 servers, UNIX/LINUX servers, and Windows XP/Windows 7 workstations and laptops.

Systems of Records Notice (SORN):

- IRS 34.037--IRS Audit Trail and Security Records System.
- IRS 36.003--General Personnel and Payroll Records
- IRS 90.001--Chief Counsel Criminal Tax Case Files
- IRS 90.002--Chief Counsel Disclosure Litigation Case Files
- IRS 90.003--Chief Counsel General Administrative Systems
- IRS 90.004--Chief Counsel General Legal Services Case Files
- IRS 90.005--Chief Counsel General Litigation Case Files
- IRS 90.007--Chief Counsel Legislation and Regulation Division, Employee Plans and Exempt Organizations Division, and Associate Chief Counsel (Technical and International) Correspondence and Private Bill File
- IRS 90.009--Chief Counsel Field Services Case Files
- IRS 90.010--Digest Room Files Containing Brief, Legal Opinions, and Digests of Documents Generated Internally or by the Department of Justice Relating to the administration of the Revenue Laws.
- IRS 90.011--Attorney Recruiting Files
- IRS 90.013--Legal Case Files of the Chief Counsel, Deputy Chief Counsel and Associate Chief Counsels
- IRS 90.015--Reference Records of the Library in the Office of Chief Counsel
- IRS 90.017--Correspondence Control and Records, Associate Chief Counsel (Technical and International)
- IRS 90.018--Expert Witness Library

Data in the System

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

A. Taxpayer:
   - entity
   - name
   - SSN/TIN
   - phone number
   - address
   - docket number
   - amount at issue in litigation
   - lien
   - judgment

- payments
- offense
- forfeiture
- income and/or penalty/interest

B. Employee:
   - name
   - login ID
   - standard employee identifier (SEID)
   - public encryption key
   - e–mail address
   - optional badge number and tax court bar number

C. Audit Trail: CC–1 relies on audit trails via Windows, UNIX/LINUX, and Oracle. The audit trail includes the following events:
   - users logon and logoff
   - change of password
   - switching accounts or running privileged actions from another account
   - creation or modification of superuser groups
   - all system administrator actions, while logged on in the security administrator role
   - all system administrator actions, while logged on in the user role
   - clearing of the audit log file
   - startup and shut down of audit functions
   - use of identification and authentication mechanisms
   - change of file or user permissions or privileges
   - remote access
   - command line changes and queries
   - batch file changes made to an application or database
   - application critical record changes
   - changes to database or application records
   - all system and data interactions concerning taxpayer data

D. Other:
   - contact data including Judge's name
   - Department of Justice Attorney name
   - names of individuals that will or have testified in a court proceeding

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

A. IRS – Electronic data received directly from the Chief Counsel Automated Systems Environment – Tax Litigation Counsel Automated Tracking System (CASE–TLCATS) application once a day to update the Counsel Automated Systems Environment–Management Information System (CASE–MIS) application, which is hosted on CC–1. The data includes:
   - CASE–TYPE
   - CASE–DATE
   - docket number
   - SSN/TIN
   - taxpayer name and address
   - assigned attorney

B. Taxpayer – Information collected directly from taxpayer correspondence containing:
- name
- address
- SSN
- public encryption key
- e–mail address
- optional badge number and tax court bar number

C. Employee – Information collected directly from employee containing:
- name
- login ID
- standard employee identifier (SEID)
- public encryption key
- e–mail address
- optional badge number and tax court bar number

3. Is each data item required for the business purpose of the system? Explain.
Yes. The data contained in the CC–1 network is critical to Counsel's ability to handle taxpayer cases, correspondence, employee training records, employee personnel data and employee work schedule data. An entity may have more than one legal case before the court with different persons associated with each case, and the taxpayer data provides the means to identify parties to the legal case and the persons associated with a particular case. Legal addresses, Judge's and Chief Counsel Attorney names are needed for contacting the parties on a case before the court. Employee IDs enable the system to identify authorized users and track access. Public Encryption Keys allow system to protect taxpayer data from unauthorized access.

4. How will each data item be verified for accuracy, timeliness, and completeness?
Information is provided by Federal Courts and IRS. Each data item is reviewed by Chief Counsel personnel for accuracy, timeliness and completeness.

5. Is there another source for the data? Explain how that source is or is not used.
No, there is no other source for the data.

6. Generally, how will data be retrieved by the user?
Data hosted on the Chief Counsel System Domain (CC–1) GSS is accessible only by authorized users on a need–to–know basis from secure CC–1 workstations, which are part of the secure domain.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is stored and is retrievable by a unique case number assigned by the U.S. Tax Court (for docketed cases) or by a unique system–generated case number (for non–docketed or refund litigation cases), and can also be retrieved by taxpayer name, SSN/TIN, and employee name.

<u>Access to the Data</u>

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

Offices of Chief Counsel personnel have access to CC–1 on a need–to–know basis as authorized by immediate managers. Systems administration is performed by a limited set of Chief Counsel staffs that have appropriate background clearances.

Role: Enterprise Administrators
Permission: This is the highest level of Chief Counsel administrators. They are responsible for the overall domain creation at the Chief Counsel enterprise level. They have full control, read, write, and execute access to all unencrypted data.

Role: Domain Administrators
Permission: These are the administrators for the entire domain. There is an administrator for each of the domains within CC–1 environment. The domains are: root domain, production domain, development domain, criminal tax domain, and a lab forest domain. This Domain Administrators group includes:

- **Role:** LAN Administrators
  Permission: this is the group where most of the network administrators belong to. They have administrator rights on the servers (e.g., file/print servers, backup servers, etc.) within their site except for domain controllers.

- **Role:** Group Policy Administrators
  Permission: these administrators are responsible for the group policy settings. They have full control, read, write, and execute access to all unencrypted data on the domains they manage.

Role: LAN Administrators
Permission: These administrators are in support roles for the servers assigned to a particular domain. They have administrator rights on the servers (e.g., file/print servers, backup servers, etc.) within their assigned area. They are also local to the specific areas of this GSS, meaning that they have access only those servers assigned (typically location specific).

Role: Group Policy Administrators
Permission: These administrators are responsible for the group policy settings.

Role: End–Users
Permission: This group is comprised of the Chief Counsel employees that are not member of the above administrative groups. They can backup their work to an assigned share drive on a CC–1 server; they have print capability to any printer within the CC–1 domain; ability to connect and logon to their assigned workstations; and access to an assigned e–mail account. They have full control, read, write, and execute access to data assigned to their user account; including encrypted data.

Role: Other IRS End–Users
Permission: There are instances where an IRS employee outside of the CC–1 GSS requires access to the data residing on the CC–1 GSS network. For these instances, the Other IRS End–User (a user not in the Chief Counsel's office) will connect to the IRS network and then access the CC–1 network via the connection that exists between the CC–1 GSS and the IRS network (depicted in the network diagram in Appendix C of the SSP). The users' rights will be predefined and given access to data that is on a need–to–know basis. An example of this would be if an attorney is working on a case that another IRS employee needs to see as part of that case. The Other IRS End–User access is always read only.

Role: UNIX/LINUX Root Administrators
Permission: These are the administrators who manage the UNIX/LINUX servers. There are no UNIX/LINUX End–users. Only the administrators noted above have direct access to the UNIX/LINUX servers. On those servers reside Oracle databases. End–users have access to the databases via COTS and in–house applications.

9. How is access to the data by a user determined and by whom?
User access requests are authorized by Chief Counsel management and by a select set of management analysts in the Office of Chief Counsel. Access requests are authorized using the Online 5081 (OL5081) system. These management analysts determine the level of access granted each user by the application. A user's access to the data terminates when it is no longer required. User's access is terminated by a system administrator upon a manager request or upon automatic account removal notice received from OL5081 system of user employment termination. 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.
Yes. CASE–TYPE, CASE–DATE, docket number, TIN, taxpayer name and address, and assigned attorney are received from the Chief Counsel Automated Systems Environment – Tax Litigation Counsel Automated Tracking System (CASE–TLCATS) application once a day to update Counsel Automated Systems Environment–Management Information System (CASE–MIS) application, which is hosted on CC–1.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Counsel Automated Systems Environment–Management Information System (CASE–MIS)

- Security Assessment and Authorization Authority to Operate – May 13, 2009
- Privacy Impact Assessment – March 23, 2009

12. Will other agencies provide, receive, or share data in any form with this system?
Data is provided by the Department of Justice, Federal Courts, Main Treasury, Labor Department, Pension Benefits Corporation, and Federal Courts. No access is given to any other agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
The Chief Counsel System Domain (CC–1) is non–recordkeeping. CC–1 is a set of applications that provides IRS attorneys and support personnel with the necessary network infrastructure to perform their jobs. Records created and/or maintained in recordkeeping systems hosted by CC–1 will be scheduled in the context of those systems and documented in the Internal Revenue Service Records Control Schedules (RCS 1.15.8–64, as applicable). Backup records can be retained for 30 years before elimination. The Chief Counsel must maintain these records to be prepared in situations where future developments or cases warrant the use of historical information that must be supplied.

14. Will this system use technology in a new way?
No. CC–1 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.
Yes. The CASE–MIS data hosted on CC–1 is used to identify individuals or groups who have filed petitions with the U.S. Tax Court or other federal courts in which the IRS is a respondent. Such cases may be identified by common case elements (i.e. tax shelter involvement, issues, etc.) in order for the Office of Chief Counsel to develop fair and consistent litigation strategy.

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.
Yes. CC–1 GSS is used to monitor individuals or groups who are party to cases docketed with the U.S. Tax Court and other federal courts. It is also used to monitor the amount of time employees devote to individual cases. Auditing capabilities are also enabled on all CC–1 servers to monitor users' activities.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. The CC–1 GSS only provides infrastructure services to authorized Chief Counsel's users.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable. The CC–1 information system is a General Support System. It does not make or track negative determinations against any party.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Although parts of CC–1 are web enabled, it does not use persistent cookies to identify web visitors.

View other PIAs on IRS.gov