

## **Counsel Litigation Support Project (CLSP) – Privacy Impact Assessment**

**PIA Approval Date – Feb. 8, 2012**

### **System Overview:**

The purpose of the CLSP project is to provide Chief Counsel Attorneys with an Enterprise Architecture (EA) approved E-Discovery Commercial Off The Shelf (COTS) tool, Clearwell. The tool helps streamline the digital investigation process by allowing them to handle more documents provided by the Modernization & Information Technology Service (MITS) E-Discovery Program Management Office (PMO) in less time while improving the accuracy of the results. This project supports one of the Chief Counsel's Strategies and Operational Priorities in managing the litigation program effectively by incorporating advanced technology into the litigation program.

### **System of Records Notice (SORN):**

- IRS 90.004—Chief Counsel General Legal Services Case Files
- IRS 90.005—Chief Counsel General Litigation Case Files
- IRS 90.009—Chief Counsel Field Services Case Files
- IRS 90.013—Legal Case Files of the Chief Counsel, Deputy Chief Counsel and Associate Chief Counsels
- 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:**

CLSP indexes the following information:

- A. Taxpayer – Information contained on IRS computers, workstations, laptops, servers and any removable media. Information on these devices consist of:
  - Taxpayer name (and spouse)
  - Taxpayer address (and spouse)
  - Taxpayer identification number (TIN) (and spouse)
  - Tax period
  - Liability amount for each tax period
  - Terms of the offer
  - All email transmissions
  - Litigation information
- B. Employee – Employee data used in this system consists of data collected on IRS computers, workstations, laptops, servers, and any removable media. This information includes USERID and password.
- C. Other – Information pertaining to Chief Counsel litigation E-Discovery requests

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

- A. IRS – Taxpayer and Employee data are obtained from the IRS E-Discovery PMO.
- B. Taxpayer – Information provided by Taxpayers in support of their case.

- C. Employee – No employee data is collected directly from the employee. Employee data comes from the IRS E–Discovery PMO.
- D. Other Federal Agencies – If information pertains to e–discovery requests.
- E. State and Local Agencies – If information pertains to e–discovery requests.
- F. Other third party resources – Other information received or other information requested through E–Discovery.

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

Yes Data elements are required in order to comply with statutory and judicial requirements of E–Discovery.

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

Each data item received is reviewed by Chief Counsel personnel for accuracy, timeliness and completeness and as required by applicable statutes and rules of procedure for e discovery.

**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 will be placed in secured electronic network folders and access to these folders will be granted to those who are assigned to work the case. Data will be retrieved by the name of the individual to whom they apply, related individuals or attorney(s) assigned, subject matters, and certain key administrative dates.

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

A unique identifier is created for each case.

**Access to the Data**

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

Counsel attorneys and/or paralegals who are assigned to work the case will have access to the data in the secured folder(s) provided by MITS E–Discovery PMO. To gain access to this application, users must submit a request through Online 5081. Other individuals may have access if authorized by applicable law that governs the disclosure of information.

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

Users have access to the data in their functional area only on a need to know basis. Access is determined and authorized by management in the Office of Chief Counsel. Applicable law may authorize access to certain information in this database to others, such as the Treasury Inspector General.

**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.**

No.

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

Not applicable.

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

No.

**Administrative Controls of Data**

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

Records has reviewed the system and find it to be non-record keeping and no further scheduling actions are needed.

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

No. No technology is used 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 Search capability of the application can be used to identify individuals or groups if present on the data being processed. This is one of the main features of the application to assist Counsel in the review, analysis, and packaging of information used in litigation.

**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 application does not provide the capability to monitor individuals or groups.

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

No. The use of this application does 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?**

Yes. The system ensures due process because the applicable due process for amending incorrect records, such as Privacy Act records is applicable to the records themselves.

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

This web-based application does not use persistent cookies or other tracking devices to identify web visitors.

[View other PIAs on IRS.gov](#)