NOTE: The following reflects the information entered in the PIAMS website.

## A. SYSTEM DESCRIPTION

*Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management*

Date of Approval: January 13, 2015 PIA ID Number: **850**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Brief Bank , Brief Bank

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

| | |
|---|---|
| Number of Employees: | Under 50,000 |
| Number of Contractors: | Under 5,000 |
| Members of the Public: | Under 100,000 |

**4. Responsible Parties:**

NA

**5. General Business Purpose of System**

The business purpose of Brief Bank is to provide Counsel attorneys a research tool and examples of how other Counsel attorneys have addressed similar issues in their Tax Court filings.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) No

6a. If **Yes**, please indicate the date the latest PIA was approved:

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)
- System is undergoing Security Assessment and Authorization

6c. State any changes that have occurred to the system since the last PIA

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. (015-000000008 Counsel Automated Legal Systems (CALS).

## B. DATA CATEGORIZATION

*Authority: OMB M 03-22 & PVR #23- PII Management*

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

| | | |
|---|---|---|
| Taxpayers/Public/Tax Systems | Yes | |
| Employees/Personnel/HR Systems | No | |
| | | *Other Source:* |
| Other | No | |

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

| TYPE OF PII | Collected? | On Public? | On IRS Employees or Contractors? |
|---|---|---|---|
| Name | Yes | Yes | No |
| Social Security Number (SSN) | No | No | No |
| Tax Payer ID Number (TIN) | Yes | Yes | No |
| Address | No | No | No |
| Date of Birth | Yes | Yes | No |

**Additional Types of PII:** Yes

| PII Name | On Public? | On Employee? |
|---|---|---|
| Login ID | No | Yes |
| Email Address | No | Yes |
| Docket Number | Yes | No |
| Vehicle Identifiers | Yes | No |
| SEID | No | No |
| Certificate/License Numbers | Yes | No |
| Passport Number | No | No |
| Financial Account Numbers | Yes | No |
| Photographic Identifiers | No | No |
| Mailing Address | Yes | No |
| Criminal History | No | No |
| Biometric Identifiers | No | No |
| Phone Numbers | Yes | No |
| Medical Information | Yes | No |
| Place of Birth | Yes | No |
| Mother's Maiden Name | Yes | No |
| IP Addresses | No | Yes |

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Middle Tiers: IRS Audit trail requirements are not implemented for these three systems. Database Tier: Database auditing is configured and audit records are captured for the following activities : use of database system privileges; statements which create, alter, delete, or rename database objects or users; session connections and failures including the usage of invalid passwords or user account, and the audit of privileged user (SYSDBA) operations. The audit trail is protected from unauthorized access. The system does not audit changes to application data including select, insert, update, or delete activities.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

| System Name | Current PIA? | PIA Approval Date | SA & A? | Authorization Date |
|---|---|---|---|---|
| Case Mis | Yes | 04/05/2012 | Yes | 04/05/2012 |

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: No If **Yes**, *specify*:

## C. PURPOSE OF COLLECTION

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

13. What is the business need for the collection of PII in this system? Be specific.

The PII in Brief Bank is necessary to complete the legal analysis required for the tax court documents and to provide useful samples for other attorneys addressing similar issues.

## D. PII USAGE

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*

14. What is the specific use(s) of the PII?

| | | |
|---|---|---|
| To conduct tax administration | Yes | |
| To provide taxpayer services | Yes | |
| To collect demographic data | No | |
| For employee purposes | No | |
| | | *If other, what is the use?* |
| Other: | No | |

## E. INFORMATION DISSEMINATION

*Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations*

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?
    If yes, please indicate means:

| | YES/NO | AUTHORITY |
|---|---|---|
| Persistent Cookies | | |
| Web Beacons | | |
| Session Cookies | | |
| Other: | | *If other, specify:* |

## F. INDIVIDUAL CONSENT

*Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights*

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

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

19a. If **Yes**, how does the system ensure “due process”?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 U.S.C.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If **No**, how was consent granted?

| | |
|---|---|
| Written consent | Yes |
| Website Opt In or Out option | No |
| Published System of Records Notice in the Federal Register | No |
| Other: | No |

## G. INFORMATION PROTECTIONS

*Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures*

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

| | Yes/No | Access Level |
|---|---|---|
| IRS Employees: | Yes | |
| Users | | Read Write |
| Managers | | Read Write |
| System Administrators | | Read Write |

| | | |
|---|---|---|
| Developers | | Read Write |
| Contractors: | No | |
| Contractor Users | | |
| Contractor System Administrators | | |
| Contractor Developers | | |
| Other: | No | |

23. How is access to the PII determined and by whom?

The access is determined by an OL5081 submitted by the requester through the business and the System Administrator.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

This is done by the business when they do their annual review.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

25a. If **Yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

Brief Bank documents are reference copies of official Chief Counsel recordkeeping material, otherwise scheduled. Brief Bank is used by IRS Chief Counsel attorneys for research purposes, and the documents can be destroyed when no longer needed for that purpose. Brief Bank documents are non-recordkeeping.

If **No**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
Documentum's security model allows projects to define groups, roles, and access controls with privileges for accessing content. The users will have to submit an OL5081 in order to grant access to the system. All users have been restricted for delete access to this system and the data is protected by using encryption backup daily. The CC-1 SSP provides the technical controls implemented at the infrastructure level.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Documentum security protects the confidentiality and integrity of information at rest through physical and logical security measures. The server is in the secure area with a lock and it's also required PIV access level to get through. There is no external access for this system. Active directory domain permissions provide logical security protection mechanisms. Encryption is used for backups that are shipped out to a remote storage location.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

None that I am aware of.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

## H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

| SORN Number | SORN Name |
|---|---|
| Treas/IRS 90;.002 | Chief counsel litigation and advice (civil) |
| Treas/IRS 90.003 | Chief Counsel litigation and advice (criminal) |
| Treas/IRS 34.037 | Audit Trail and Security Records System |

## I. ANALYSIS

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

| | |
|---|---|
| Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated) | No |
| Provided viable alternatives to the use of PII within the system | No |
| New privacy measures have been considered/implemented | No |
| Other: | No |

32a. If **Yes** to any of the above, please describe:

NA