

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: 08/01/2014 PIA ID Number: 1003

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):

Counsel Automated Systems Environment-Management Information Systems, Tax Litigation Counsel Automated Tracking System, CASE-MIS, TLCATS

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: Not Applicable

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

CASE-TLCATS is a key management information system used by the Office of Chief Counsel to track all aspects of Tax Litigation cases. It is an online interactive and batch processing system that allows Chief Counsel personnel to store and retrieve case data throughout all phases of the Tax Litigation process, allowing for coordination Nationwide. CASE-TLCATS also tracks case events and due dates for items due to the taxpayer, US Tax Court, Federal District Courts, US Court of Federal Claims, Federal Courts of Appeals, and the Supreme Court. The application tracks trial calendars and provides the U.S. Tax Court, through the Chief Counsel, with a status of those cases on each trial calendar. CASE-TLCATS provides the Chief Counsel Business Unit (BU) management with case statistics at various organizational levels. CASE-TLCATS provides outputs to the Appeals Centralized Database System (ACDS) and the Counsel Automated Systems Environment - Management Information System (CASE-MIS). Due process for the cases is provided pursuant to 26 USC and the rules of the tax court as applicable.

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) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 07/05/2011

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) No
 - System is undergoing Security Assessment and Authorization Yes
-

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

NA

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'. 015-45-01-14-02-2367-00-315-180

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

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

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)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

- Entity (e.g. corporation name, etc.) and persons associated with case
- Name
- SSN
- EIN
- Address
- Tax Court Case Number
- CASE-TYPE
- CASE-DATE
- Docket Number

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

<http://www.irs.gov/pub/irs-wd/00-0075.pdf> <http://www.law.cornell.edu/uscode/text/26/6109> Section 7801 and 7803 of the Internal Revenue Code

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

The system does allow for the collection of SSNs; however, IRS and Congress have not provided for an alternative means to identify taxpayers.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

No strategy that can be implemented exists currently in Applications Development to eliminate the use of SSN's. Technical and economic feasibility considerations are being analyzed to reduce the amount of SSNs used within TLCATS.

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.

All Audit Log Information is captured on the mainframe where CASE-TLCATS resides. The Audit Information captured is as follows: • Logon/Logoff (The SEID is the only element to identify the user for the system Audit Trail.) • Change of password • Creation or modification of super users • Startup/shutdown • Changes to data

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

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

US Tax Court	No		No	
Circuit Court	No		No	
District Court	No		No	

b. Other federal agency or agencies: Yes

If Yes, please list the agency (or agencies) below:

U.S. Tax Court, Federal Court or District Court – Taxpayer name, SSN/EIN, Judge's name, and Court Case Number, (Related Parties) Entity or Persons associated with case.

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

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 data elements are required to perform litigation activities with the courts. An entity may have more than one legal case before the court with different persons associated with each case. The taxpayer data provides the means to identify parties to the legal case and the persons associated with a particular case. Attorney's names are needed for contacting the parties on a case before the court.

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	<u>Yes</u>
To provide Taxpayer Services	<u>Yes</u>
To collect Demographic Data	<u>No</u>
For employee purposes	<u>No</u>

If other, what is the use?

Other:	<u>No</u>	<u>_____</u>
--------	-----------	--------------

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

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

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	_____	_____

If other, specify:

Other: _____

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

18a. If Yes, how is their permission granted?

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 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

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 _____
Website Opt In or Out option _____
Published System of Records Notice in the Federal Register _____
Other: _____

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:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?**23. How is access to the PII determined and by whom?**

On-Line 5081 Management Approval transaction processing system. All managers of record established for their specific employees.

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

Manual and system built in checks on field input.

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? No

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.

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.

The typical output generated by the GSS-21 GSS mainframes is the audit logs that are executed and produced on a daily/weekly basis. The system audit output logs are retained on the mainframe and are backed up nightly as part of the normal backup procedures. Audit logs are maintained and destroyed, as defined by IRM 1.15.19, Records Control Schedule. Storage media is sanitized (e.g., overwritten, degaussed, or destroyed) prior to reuse or release. Storage media is protected from magnets, liquids, and other environmental hazards. Storage media removed from the office are afforded the same protection as paper documents containing the same information. CASE-TLCATS is unscheduled. A request for records disposition authority for survey data is currently being drafted with the

assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions will be published in IRS Document 12990, Records Control Schedule and item number to be determined. Until a schedule is established and approved, all records will be retained.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The admin and Technical security controls implemented on TLCATS are documented in the FISMA SSP.

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

GSS-21 protects data at rest as follows: Desktops/Mobile Devices/Mobile Media. All IRS data stored on deployed user desktops/laptops is protected through the use of whole disk encryption as deployed throughout the IRS enterprise. All mobile devices or media used to store SBU data are also encrypted using IRS approved encryption. Back Up Tapes. GSS-21 uses the Encryption Key Manager (EKM) digital certificate process to encrypt backup tapes for offsite storage. EKM is a part of the IBM Java run time environment and uses IBM Java security components for the cryptographic capabilities. IBM Mainframe. IRM 10.8.1.5.6 (12) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. GSS-21, in accordance with the IRM, has employed the following due diligence methods for protecting the SBU data that resides on the mainframe: GSS-21 shares DASD, RACF and SMS managed storage. GSS-21 enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. GSS-21 reports are printed in accordance with business need. Reports are handled appropriately in accordance with organizational policies. GSS-21 has had a risk assessment conducted. Compliance Services has previously completed a Security Impact Analysis and is conducting a new SIA as part of the current SA&A cycle. The GSS-21 SSP is being updated as part of the current SA&A to reflect the encryption utilized by the GSS to protect SBU data. Physical security is inherited for GSS-21 at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

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? Yes

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

Annual assessment on the procedures, security and policies implemented on the application. RACF enforces the policies to ensure the safeguards for the PII.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?

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.

SORNS Number

SORNS Name

Treasury/IRS 90.16 Chief Counsel Systems Environment (CASE)

Treasury/IRS 34.037 IRS Audit Trail & Security Records

Treasury/IRS 44.001 Appeals Case File

Treasury/IRS 44.003 Appeals Centralized Data Systems (ACDS)

Comments

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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

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

NA

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