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 Submission: Feb. 7, 2012 PIA ID Number: **152**

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):

Large Business and International Workloard Identification System, LWIS

2a. Has the name of the system changed? Yes

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

Large and Mid–Sized Business Workload Identification System

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

The Large Business and International Division (LB&I) Workload Identification System (LWIS) is an Internal Revenue Service (IRS) Minor Application that has been in operation since 2001. It is primarily used by IRS Industry Planning and Special Programs (PSP) Analysts to identify LB&I Business tax returns for field group managers that were selected for potential audit, resulting in the delivery of the tax returns to the LB&I revenue agents. The LWIS application is a collection of custom, IRS–developed software applications that are used for entering, retrieving, or deleting data on a Microsoft SQL 2005 database. Functionality within the LWIS application is the LB&I Electronic Classification System (LECS), which allows revenue agents to review returns and complete a classification sheet. The classification sheet is used to determine whether the audit should take place and would include any preliminary findings. Management and Collaboration (CMC), a subsystem of LWIS, is a documentation storage system for LWIS documents that were selected for audit and classifies them as to their audit potential. CMC is an enhancement of LECS and provides a more thorough classification review. LWIS is also integrated with the LB&I Image Net (LIN), a separate application that stores returns as .pdf images. If LIN has a file of the return in the .pdf file format, LWIS points the revenue agent to the file through a hyperlink. LWIS contains the following Personally Identifiable Information (PII) for each business entity: Employer Identification Number (EIN); address (city, state, and zip code [plus 4]); and Master File Account tax information elements (e.g., Industry Code, Tax Period Return Filed (TXPD), Audit Information Management System (AIMS) information, historical tax event codes and dates, and Disaster Victim Status).

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: 04/29/2009

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

LWIS has moved from being Access–based to SQL in webpages

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'. 015–45–01–13–02–244–00

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

Additional Types of PII: Yes

PII Name	**On Public?**	**On Employee?**
EIN	Yes	No

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

Business taxpayer information in LWIS/LECS is taken from returns filed on Forms 1120, 1120S, 1120F and 1065. The data in the LWIS system includes the Employer Identification Number (EIN) city location; state; zip code (plus 4); Master File Account (tax information elements include: Industry Code, Tax Period Return Filed (TXPD), Audit Information Management System (AIMS) information, historical tax event codes and dates, Disaster Victim Status).

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.)

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

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

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 auditing is performed at the server level and is the responsibility of the MITS–30 GSS.

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
Audit Information Management System Reference (AIMS–R	Yes	08/29/2001	Yes	05/01/2009
Specialist Referral System (SRS–2	Yes	05/05/2009	Yes	06/16/2009
LB&I Image Network (LIN)	No	05/05/2009	No	06/16/2009

b. Other federal agency or agencies: No
If Yes, please list the agency (or agencies) below:

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.

LWIS uses each data item to identify returns for team managers for LB&I Form 1120, 1120S, 1120F and 1065 returns on an as needed basis.

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	No	
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

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		
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

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? Not Applicable

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

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:	Yes	
Users		Read Only
Managers		Read Only
System Administrators		Read Write
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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?

Users are authorized to use the system by their managers via the On–Line 5081 (OL5081) system.

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

Authoritative data has been validated in the Business Master File (BMF) system prior to sending data to AIMS, which then sends the data to the LWIS application. Authoritative data has been validated in the LB&I Image Network (LIN) system prior to sending data to LWIS.

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.

LWIS data is approved for destruction under NARA Job No. N1–58–88–4, and published under IRM/Records Control Schedule 1.15.23 Tax Administration – Examination, Item 48. However, in reviewing LWIS–related recordkeeping practices for completion of this PIA, system owners and the IRS Records Office determined that a re–evaluation of 1.15.23, item 48 descriptions and disposition authorities are in order. LB&I and the Records Office will work together to validate and potentially update the item to better fit current data collection activities and maintenance needs, and the current electronic recordkeeping environment.

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.

The MITS–24 and MITS–30 GSSs protect LWIS data at rest as follows: Back Up Tapes: MITS–24 and MITS–30 GSSs uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140–2 validated encryption. Application Servers: 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. The MITS–24 and MITS–30 GSSs environment, in accordance with the IRM, has employed the following due diligence methods for protecting the LWIS PII data that resides on the servers:

- LWIS does not utilize any shares or shared drives.
- LWIS enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties.
- LWIS does not routinely print any documents. If required, printing is limited to the specific reason for printing any document.
- LWIS has had a risk assessment conducted. Security Assessment Services has previously completed a Security Impact Analysis and will conduct a new SIA as part of the current SA&A cycle.
- The LWIS SSP is being updated as part of the current SA&A to reflect the encryption utilized by MITS–24 and MITS–30 GSSs environment to protect PII data. Physical security is an inherited control by LWIS at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

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

The LWIS application uses Electronic File Transfer Utility (EFTU) in conjunction with Tectia to provide the required cryptographic protections for data in flight or in transition that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

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.

Continuous Monitoring (eCM) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

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)*?

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 24.046	Business Master File
Treasury/IRS 34.037	Audit Trail and Security Records System
Treasury/IRS 42.008	Audit Information Management System
Treasury/IRS 42.021	Compliance Programs and Project Files

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:

N/A

View other PIAs on IRS.gov