A. SYSTEM DESCRIPTION

1.   Enter the full name and acronym for the system, project, application and/or database. Large Business and International Workload Identification System, LWIS, LWIS (LECS/CMC/CBF)

2. Is this a new system? No

> 2a. If **no**, is there a PIA for this system?   Yes
>
>> If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.
>>
>> LWIS, PIAMS # 1471
>>
>>
>> Next, enter the **date** of the most recent PIA.   10/5/2015
>>
>> Indicate which of the following changes occurred to require this update (check all that apply).

Yes	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

> Were there other system changes not listed above?   No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system?   No

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

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 Practice Area 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. In August 2018, the systems will also process LB&I's individual tax returns. Content Management and Collaboration (CMC), a subsystem of LWIS, is a system that uses analytical procedures and enhanced filters for real-time and continuous risk assessment of returns. Risk assessment information is included in the CBF from CMC. LWIS is the return ordering system for the returns. Case Built File (CBF) is a document repository for use by field agents. LWIS is integrated with 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. LIWS is integrated with LB&I Issue Management System (IMS) to deliver UIL and SAIN description information and work papers. LWIS contains the following Personally Identifiable Information (PII) for each business entity and individual: Employer Identification Number (EIN); Social Security Number (SSN); 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).

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

   6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

   If **yes**, check who the SSN (or tax identification number) is collected on.

   Yes   On Primary   No   On Spouse   No   On Dependent

   If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

   Yes   Social Security Number (SSN)
   Yes   Employer Identification Number (EIN)
   Yes   Individual Taxpayer Identification Number (ITIN)
   No   Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
   No   Practitioner Tax Identification Number (PTIN)

   Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

   System databases store SSN/EIN information that is inherited from AIMS. The system displays the EIN/SSN as needed within the applications. There is no ability to search, add or modify SSN/EIN information. The project is implementing NTIN Checking into all the modules. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates?   Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
Yes	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

.

6d. Are there other types of SBU/PII used in the system?   Yes

    If **yes**, describe the other types of SBU/PII that are applicable to this system.   Business taxpayer information in LWIS/LECS/CMC/CBF 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). Individual taxpayer information in LWIS/LECS/CMC/CBF is taken from returns filed on Forms 1040, 1040EZ, 1040NR and 1040NR-EZ. The data in the LWIS system includes the Social Security Number (SSN); 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).

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner?   Yes

---

B.1 BUSINESS NEEDS AND ACCURACY

---

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

    Use is limited to projects classification and workload delivery systems. LWIS uses each data item to identify returns for team managers for LB&I Forms 1040, 1040NR, 1040NR-EZ, 1120, 1120S, 1120F and 1065 returns on an as needed basis. The LWIS application is a collection of custom, IRS-developed software applications that are used for entering, retrieving, or deleting data on a 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

    Data used by the application is from other sources. The data received is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system?   Yes

   9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual?   No

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies?   Yes

   11a. If **yes**, does the system receive SBU/PII from IRS files and databases?   Yes

   If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Audit Information Management System (AIMS)	Yes	10/15/2015	Yes	08/13/2015
LB&I Image Network (LIN)	No		No	08/13/2015

   11b. Does the system receive SBU/PII from other federal agency or agencies?   No

   11c. Does the system receive SBU/PII from State or local agencies?   No

   11d. Does the system receive SBU/PII from other sources?   No

   11e. Does the system receive SBU/PII from **Taxpayer** forms?   No

   11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)?   No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII?   Yes

   12a. Does this system disseminate SBU/PII to other IRS Systems?   Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
LB&I Taxpayer Registry (LTR)	Yes	03/16/2016	Yes	08/24/2015
Integrated Management System (IMS)	Yes	08/04/2016	Yes	04/30/2014

Identify the authority and for what purpose?   Systems are authorized to operate for the purpose of classifying returns and performing workload delivery.

12b. Does this system disseminate SBU/PII to other Federal agencies?   No

12c. Does this system disseminate SBU/PII to State and local agencies?   No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors?   No

12e. Does this system disseminate SBU/PII to other Sources?   No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels?   No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?   No

15. Does the system use cloud computing?   No

16.   Does this system/application interact with the public?   No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information?   No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.
Tax return information is inherited from AIMS. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?   No

18b. If no, why not?   Tax return information is inherited from AIMS> LB&I does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Tax return information is inherited from AIMS. There are no changes made to data received. The process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process."

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).   IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees?   Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees?   Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	Yes	Administrator	Low

21a. How is access to SBU/PII determined and by whom? Permissions are granted to systems via an approved OL-5081. A potential user must submit a request for access via IRS OL5081 to their local management for approval consideration. Users are not permitted access without a signed 5081 form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the OL5081 form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. Users are assigned to specific modules of the application and specific roles within the modules and accounts follow the principle of least privilege which provide them the least amount of access to Pii data that is required to perform their business function after receiving appropriate approval. All actions performed by the users in application have been assigned to them from higher IRS management and are limited to the duties assigned to them.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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.

All records housed in the LWIS system will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedules (RCS) 23, Item 48, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)?   Yes

    23a. If **yes**, what date was it completed?   2/5/2013

23.1 Describe in detail the system s audit trail.   The application is in the operations and maintenance phase and adequate engineering principles are being utilized in accordance with security engineering principles. The IRS IT Cybersecurity organization provides support throughout the security certification and accreditation process. The LWIS maintenance and development requires system-security features to be compliant with all applicable federal government and IRS policies, standards and guidelines. LWIS operating system security requirements include system audit trails, user authorization and authentication control via Active Directory, and user level access control for data via specific roles and privileges. End users have accounts created that permit limited access to query the application. Because the application only grants limited access, users are strictly prohibited from inputting any information to the application, other than Classification Forms and case related documents. The systems rely on validity checking being performed by AIMS and LIN and the NTIN process. No search is allowed per taxpayer/TIN/SSN/Address. The users only know what taxpayer after management has assigned the return to them. Systems have full audit trails on who assigned, when, to whom, and result.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

    24b. If **yes**, Is the test plan in process or completed: In Process

       If **in process**, when is the test plan scheduled for completion?   7/30/2018

       24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
All systems require OL5081 for access. System handles LB&I inventory. Systems use Integrated Windows Authentication which obtains SEID from cached Active Directory information, OL5081 and case assignment. This validates who you are and then that identify is used throughout the system, including roles and membership. Roles are defined by each application's needs. Systems retain data based on IRM directives. System have internal auditing implemented and system auditing is handled by GSS-30. Employees take various training such as UNAX. User guides are updated with each release and FAQs share additional information and training sessions are held as needed with end users. Negative TIN checking is controlling confidentiality and are in process of implementation. User roles are tied to specific available actions within the systems. User Acceptance Testing is conducted to validate the requirements of the system.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing?   Yes
    25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use
        Questionnaire or Form 14665, SBU Data Use Request?   Yes

    If **yes,** provide the date the permission was granted.   1/11/2017

    25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified
        (SBU) Data Policy: Protecting SBU in Non-Production Environments?   Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

    26a. IRS Employees: Not Applicable
    26b. Contractors: Not Applicable
    26c. Members of the Public: More than 1,000,000
    26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights
guaranteed by the First Amendment?   No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11
Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than
    IRS employees in the performance of their duties, or to the person to whom the information pertains
    or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report