

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: November 20, 2014

PIA ID Number: **876**

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):

Department of Labor Standards Enforcement, DLSE

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: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

DLSE is primarily used to process information submitted by taxpayers from the California garment, agricultural, car washing and polishing industries (companies). DLSE automates the research for federal employment tax requirements in an accurate and timely fashion. These industries (companies) taxpayers complete Form 8821 and send it to the IRS for processing. These industries must be cleared by the IRS in order to successfully operate. If the industry (company) taxpayer is in compliance with federal requirements, a letter is provided to the taxpayer to be presented to the state.

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: 2/20/2009 12:00:00 AM

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

None.

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

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)	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. What is the business purpose for collecting and using the SSN?

To identify the business owner.

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.)

IRC 6109.

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

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed.

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

There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

Describe the PII available in the system referred to in question 10 above.

Taxpayer – The data stored in DLSE contains: • Taxpayer Identification Number (TIN) • Federal Employer Identification Number (EIN) or Social Security Number (SSN). The taxpayer's SSN is used to identify who is the owner of the business if they file with an EIN. If they are a sole proprietor, an SSN is the only identifying number used. DLSE also may contain: • Business name • Address • License # (if applicable) • Telephone numbers • Tax year • Taxpayer name • Taxpayer address • Appointee information • Business/Industry info • Case Status • Case type • Date entered/received Case results

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.

The DLSE application itself does not require a separate login. The user is granted a shortcut to the application on his or her desktop so that logging onto the IRS network equates to access to DLSE. The following IRS network user activities are logged and the data reviewed by the Modernization and Information Technology Services (MITS) security team on an ad hoc basis: • logon/logoff by User ID • password change • create/delete/open/close file name • program initiation • all Systems administrator (SA) and database administrator (DBA) actions.

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: No
- b. Other federal agency or agencies: No
- c. State and local agency or agencies: Yes
If **Yes**, please list the agency (or agencies) below:
State of California Department of Labor.
- d. Third party sources: No
- 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.

We report to the State of California Department of Labor the employers that are deemed to be compliant and non-compliant in filing and paying their employment taxes.

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>

Other: No

If other, what is the use?

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.) Yes

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)	No		
State and local agency (-ies)	Yes	The State of California Department of Labor.	Yes
Third party sources	No		
Other:	No		

** 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? No

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"?

If the taxpayer is in compliance with federal requirements, a license is provided giving the taxpayer the authority to operate. Negatively affected parties may respond to a negative determination prior to final action by resubmitting the required form.

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.

ID	Form Number	Form Name
4404	8821	Tax Information Authorization
4405	941	Employer's Quarterly Federal Tax Return
4406	945	Annual Return of Withheld Federal Income Tax
4407	940	Employer's Annual Federal Unemployment (FUTA) Tax Return

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 Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Write</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?

Approval for access is determined by the supervisor in accordance with the OL5081 process. The system administrator would then add the user to the global access group.

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

DLSE users manually compare the reports to ensure accuracy, timeliness and completeness of each data item on a weekly basis. A monthly Embedded Quality Review System (EQRS) quality review also takes place.

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.

DLSE data is approved for destruction 3 years after the end of the processing year under National Archives and Records Administration (NARA) Job No. N1-58-09-15. Disposition instructions are published in IRS Records Control Schedule (RCS) Document 12990 under RCS 28 for Tax Administration - Collection, item 153.

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.

All records are kept in individual files that are placed on a wall so that the PII information is secure.

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

NA

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.

The records are monitored to ensure no unauthorized access.

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*)? Yes

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 24.046	BMF
treas/ies 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)	<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