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: March 31, 2015 PIA ID Number: **1183**

1. Enter the full name and acronym for the system, project, application and/or database. SPIIDE DLP System, DLP

2. Is this a new system? Yes

2a. If **no**, is there a PIA for this system?

If **yes**, enter the full name, acronym, and milestone of the most recent PIA.

Next, enter the **date** of the most recent PIA.

Indicate which of the following changes occurred to require this update (check all that apply).

No	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? _

If yes, explain what changes were made.

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
Yes	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

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

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 purpose of the IRS Securing PII Data Extracts (SPIIDE) project is to implement Data Loss Prevention (DLP), providing the IRS the ability to prevent the exfiltration of Agency-held or existing Personally Identifiable Information (PII) and Sensitive Agency Information (SAI). DLP is capable of monitoring network traffic for outgoing PII/SAI, flag traffic that violates security policies, and facilitate response actions.

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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

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

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

The SPIIDE DLP System is designed specifically to detect unencrypted SSNs that are being transmitted outside of the IRS IT boundary via email or web interface. The SSNs detected are stored in the DLP System database which is encrypted using FIPS 140-2 approved algorithms. The SSNs can be taxpayer or IRS employee PII. The DLP System also has a blocking feature which will prevent detected SSNs from leaving the IRS IT boundary. There is no mitigation plan to eliminate the use of SSNs as the system is designed to detect them. However, access to the DLP event database is strictly controlled with only the minimum number of IRS personnel having access.

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

If **yes**, specify the information.

Selected	**PII Element**	**On Primary**	**On Spouse**	**On Dependent**
Yes	Name	Yes	Yes	Yes
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No

Yes	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
Yes	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
Yes	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	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
No	Tax Account Information	No	No	No
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? No

.

6d. Are there other types of SBU/PII used in the system? No

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

No PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a

No SSN for tax returns and return information is Internal Revenue Code Section 6109

Yes 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

If the answer to 6f is **No**, verify the authority is correct with the system owner and then update the answer to 6f.

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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The SPIIDE DLP System was purchased and deployed by the IRS to help prevent the illegal or unintentional dissemination of PII (specifically SSNs) outside the IRS. The system detects unencrypted SSNs leaving the IRS boundary via email or web transactions. Once detected the System can prevent the delivery of the unencrypted SSN before it leaves the boundary. The DLP System generates an "event" each time a SSN is detected and the information associated with the event (detected SSNs, IRS employee data, offending email etc.) is stored in the DLP encrypted database. DLP Event Responders review the event to determine if it was genuine and refer the event to appropriate authority for further action. Event data access is limited to Event Responders only and cannot be accessed remotely.

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.

The initial scope of the DLP solution is to monitor for Social Security Numbers (SSN) that exit the network via email, web or Internet egress points. Policy violations will be captured by geographically and logically dispersed sensors. The sensors will encrypt and send the captured data elements back to the central management system. The central management system utilizes an Oracle database to store policy violations and associated data as an encrypted file. Access control policies will restrict users who have access to the system as well as users who have access to PII/SAI data. It will be important to verify that the numbers within an email are actually SSNs in order to execute appropriate incident response procedures.

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? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	**SORNS Name**
34.037	Audit Trail and Security Records

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles.

NA

E. INCOMING PII INTERFACES

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? 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, cloud, 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? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
All IRS employess are notified as a condition of employment that their email and web traffic may be monitored. Additionally, each time an employee logs into the IRS IT infrastructure they receive a pop up message that states that the use of government computing services comes with the knowledge that all electronic communications may be monitored. This electronic communications monitoring condition of employment is not voluntary and cannot be opted out of.

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.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):

18b. If no, why not? The DLP System is designed to detect inadvertent or possibly illegal dissemination of unencypted SSNs leaving the IRS IT Boundary. The SSNs captured by the DLP System are stored in an encrypted database. The System is in place to PREVENT the dissemination of unencrypted taxpayer SSNs to unauthroized personnel outside the IRS. The DLP System does not monitor inbound message traffic or email from the general public. It only monitors outgoing IRS email and web traffic. IRS employees give their consent to monitoring of email and web communications as a condition of employment. There is no direct consent given by employees to monitoring by the DLP System.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Due process is not applicable to the public in general as the system does not "use" the event information to interact with the tax paying public in any way. IRS employees and contractors using IRS email and web services may face discplinary action for the misuse of SSNs. All IRS employees will be given the opportunity to defend their actions before a final determination is made. Contractor employees will be afforded any rights granted within the regulations that cover the specific contract they are working under.

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? Yes

Contractor Employees?	**Yes/No**	**Access Level**	**Background Invest.**
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? The DLP PMO determines who may be granted access to the system and the role they will have. Role based access requests has been developed in the OL5081 System. The DLP System roles are desgined with the concept of least privilege and only the events specifically referred to a role may be viewed by the Event Responder. The DLP PMO will reside within CyberSecurity Operations once the system is fully operational.

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?

Yes

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? No

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.

22b. 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.

SPIIDE (DLP) is unscheduled. The system is preparing to deploy; the Business Owner will work with the IRS Records and Information Management (RIM) Program Office to determine and draft for National Archives approval the appropriate disposition/retention of captured SSNs, and the names and email addresses of employees identified as having sent SSN data through email or web traffic. SPIIDE will notify the Office of Privacy when a RCS schedule is approved. Until that time, no records may be destroyed. It is estimated that system data will need to be kept for 7 years to comply with law enforcement requirements.

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? 10/17/2014 12:00:00 AM

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

23.1 Describe in detail the system s audit trail. All DLP Event data is stored in the DLP System's encrypted Oracle database. Every event contains a unique identifying number. All user notes, access, edits, and changes are logged either in the event data profile itself or within the DLP System internal audit system. In addition, all system changes including server adjustments, policy additions or changes, user and role definitions/changes are captured in the DLP audit trail and by the ESAT team. The project is also working with the ESAT team to capture audit trails of event metadata to ensure DLP Event data is not compromised.

J. PRIVACY TESTING

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

24c. If **no**, please explain why.

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

If **in process**, when is the test plan scheduled for completion? 5/15/2015 12:00:00 AM

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?
The DLP System has completed application, integration testing and most of the functional testing. Strict accountability is achieved through the role based access via OL5081. OL5081 has not been fully implemented and tested yet. Functional testing has been conducted to ensure only the data required to identify the sender of unencrypted SSNs is collected by the system.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

24b.2. If **completed**, were all the Privacy Requirements successfully tested?

If **no**, please explain which Privacy Requirements were not tested and why?

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

If **yes**, please describe the outstanding issues.

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 13471 Live Data Request? Yes

If **yes,** provide the date the permission was granted. 10/2/2014 12:00:00 AM

If **no**, explain why not.

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 IT Security, Live Data Protection Policy? Yes

If **no**, explain why not.

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Not Applicable
26d. Other: No

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

M. CIVIL LIBERTIES

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

27a. If **yes**, explain the First Amendment information being collected and how it is used.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). No
The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q 7) No
There is a statute that expressly authorizes its collection. (Identified in Q6) No

27c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges?

If **yes**, explain the determination process. Consult with IRS General Legal Services to complete this section.

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

If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? Yes

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. The system's purpose is to "monitor" data moving out of the IRS network protection and can be focused on individuals or groups. But this functionality is ONLY intended to be used by law enforcement, i.e. TIGTA, CI, etc.

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

If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required.

30a**.** If **no**, accounting of Disclosures risk noted. Contact *Disclosure* to develop an accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

30b. If **N/A**, explain the Exemption and/or Disclosure s response.

End of Report