Date of Approval: 11/20/2025
Questionnaire Number: 2596

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Symantec Data Loss Prevention

Acronym:

SDLP

Business Unit

IT - Cybersecurity

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Symantec Data Loss Prevention (SDLP) system provides the IRS the ability to prevent the accidental loss or disclosure of taxpayer information, existing Personally Identifiable Information (PII), Federal Tax Information (FTI) and Controlled Unclassified Information (CUI). DLP is capable of monitoring email and internet communications for outgoing PII/CUI and prevent the loss or disclosure of unprotected PII/CUI information. The Symantec Data Loss Prevention system is owned and operated by the IRS. Co-owners/administrators/contractors involved are Computer Security Incident Response Center (CSIRC), Counter-Insider Threat (CInT), Treasury Inspector General for Tax Administration (TIGTA), Privacy, Governmental Liaison, Disclosure (PGLD), Safeguarding Personally Identifiable Information Data Extracts (SPIIDE), Criminal Investigations (CI), Small Business/Self-Employed

(SB/SE). This system is located on premises at IRS data centers. A Data Loss Prevention (DLP) tool helps satisfy the following NIST SP 800-53 items: AC-4 (Information Flow Enforcement), SI-4 (System Monitoring), SC-12/SC-28 (Data Protection and Encryption), and AU-2/AU-12 (Auditing and Log Management). It supports the IRS's mission to fulfill IRMs 10.5.1.2.2.1 (Privacy and Information Protection) which states the mission of "Protect the privacy of sensitive but unclassified (SBU) data for taxpayers and personnel, including personally identifiable information (PII), such as federal tax information (FTI, referred to in this IRM as tax information), tax return, financial, and employment information regardless of format.". Symantec DLP communicates over Transport Layer Security (TLS) encrypted channels. The Symantec DLP Detection Servers send detected events securely to the Enforce Server via TLS, and endpoint agents communicates with detection servers using encrypted transfers. Access to the system is provided via privileged entitlements. The Symantec DLP database is hosted in the Exadata platform and encrypted using AES-256.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

The scope of the DLP solution is to monitor for Social Security Numbers (including Taxpayer Identification Numbers) that exits 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, which utilizes the database to store policy violations and associated data alongside related encrypted files. Access control policies restrict users who have access to the system as well as users who have access to Personally Identifiable Information or related sensitive data. It is important to verify the numbers within the collected data are SSNs/TINs to execute appropriate incident response procedures. Data Loss Prevention SPIIDE (DLP) is scheduled (DAA-0058-2013-0010). Once an investigation is completed regarding possible policy violation, all related records housed in the DLP system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained 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 Schedule (RCS) 17, Item 35, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Agency Sensitive Information
Alien Registration Number
Citizenship or Migration Status
Credit Card Number
Criminal Investigation Information
Criminal Record
Email Address
Employer Identification Number
Employment Information
Family Members
Federal Tax Information (FTI)
Financial Account Number
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
Official Use Only (OUO) or Limited Office Use (LOU)
Passport Number
Preparer Taxpayer Identification Number (PTIN)
Procurement Sensitive Data
Protected Information
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number

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

PII for personnel administration - 5 USC
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system? (Number)

3

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

5828

4.12 What is the previous PCLIA title (system name)?

Safeguarding Personally Identifiable Information Data Extracts (SPIIDE)
automated Data Loss Prevention (DLP) System, DLP

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Expired PCLIA

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

Yes

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

SEC-1

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

211328

10 If this system discloses any PII to any third party outside the IRS, 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?

No

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

Personally Identifiable Information (PII) that are collected, processed, and discarded relating to tax, employee, or personnel information are strictly disclosed to Internal Revenue Service (IRS) employees and contractors that support with investigation of alerts generated by the system, operations and maintenance relating to the Symantec Data Loss Prevention (SDLP).

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Individuals are restricted to access and modify collected any information, with the exclusion of administrators, in the system as this would interfere with IRS DLP operation, pose a risk to the security posture, and violate confidentiality, integrity, and availability relating to information security.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

a. IRS Employees
    i. Users: Read Write
    ii. Managers: Read Write
    iii. System Administrators: Administrator
b. IRS Contractor Employees
    i. Contractor Users: Read Write
    ii. Contractor System Administrators: Administrator

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

Privacy Act Statement not used.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Under 50,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Under 5,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Under 100,000

22 How is access to SBU/PII determined and by whom?

The DLP Project Management Office (PMO) determines who may be granted access to the system and the role they will have. Role-based access requests have been developed in the OL5081 System. The DLP System roles are designed with the concept of least privilege and only the events specifically referred to a role may be viewed by the Event Responder.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

Yes

24 Explain any privacy and civil liberties risks related to privacy controls.

All controls in place are to restrict access to collected information to only authorized personnel on a need-to know basis, including Symantec Data Loss Prevention (SDLP) administrators and users such as analysis for investigating possible violation of Internal Revenue Manual (IRM). Collected information is not disseminated externally to the system, except for audit trail purpose as required by the IRS policies.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

All DLP Event data is stored in the DLP System's encrypted 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 Enterprise Security Audit Trails (ESAT) team.

27 Does this system use or plan to use SBU data in a non-production environment?
Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.
Yes

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
EXA DATA - EOPS
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
TLS 1.2 or higher

Interface Type
IRS Systems, file, or database
Agency Name
HP DL 360 G7 w/ Endace NIC
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP) - Passive

Interface Type
IRS Systems, file, or database

Agency Name
Email Prevent (IBR and INET)
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
TLS 1.2 or higher

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
This SORN allows IRS to record unauthorized activities relating to accessing and disclosing SBU information that is forbidden by IRS policy and detect unauthorized electronic communication using IRS systems in violation of IRS security policy. Additionally, this SORN exempts these records and systems to disclosed to the public under 5 U.S.C. 552a(k)(2).

Records Retention

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
Information Technology
What is the GRS/RCS Item Number?
17 Item 35
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
Data Loss Prevention (DLP) System. The Data Loss Prevention tool blocks outbound disclosure of Personally Identifiable Information (PII) and logs incidents temporarily within the application console for review and remediation. This tool helps IRS employees avoid inadvertent IRM violations and increases their awareness about safe practices. System contains details of any PII data breach event. These details include sender information, recipient email address, and the email or web traffic contents of the potential incident. (Job No. DAA-0058-2013-0010-0001)

What is the disposition schedule?

AUTHORIZED DISPOSITION Cut off upon close of event. Delete/Destroy 90 days after cutoff or when no longer needed for administrative, legal, audit, or other operational purposes, whichever is later. Incidents which are referred to incident-review organizations (i.e. PGLD, CSIRC, and TIGTA) may require longer DLP retention, pending the completion of any necessary data sharing. At that point, incident information will follow the review organization's retention policies.

Data Locations

What type of site is this?

Environment

What is the name of the Environment?

SPIIDE Data Loss Prevention (DLP) Data-In-Motion (DIM) Web Prevent

What is the sensitivity of the Environment?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the Environment.

Monitor and prevent potentially unauthorized web traffic from traveling outbound from the IRS network.

What are the incoming connections to this Environment?

The web proxy sends outbound web traffic data to the Web Prevent VM, which initially monitors for potentially unauthorized web traffic leaving IRS network. The VM is managed through the Enforce Management Console.

What are the outgoing connections from this Environment?

After determining a web traffic is unauthorized based on policies established through Enforce Management Console, the traffic is blocked from going outbound from the internal IRS network after the policies are pushed and updated on the web prevent VM.

What type of site is this?

System

What is the name of the System?

SPLUNK

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

Please provide a brief description of the System.

Retain system records for auditing as specified in the IRM Part 10 Chapter 8, under the AU control family.

What are the incoming connections to this System?

There are no incoming connections from SPLUNK to SDLP.

What are the outgoing connections from this System?

Application and system logs are sent to Splunk via TCP connection for audit record compliance.

What type of site is this?

Environment

What is the name of the Environment?

SPIIDE Data Loss Prevention (DLP) Data-In-Motion (DIM) Email Prevent

What is the sensitivity of the Environment?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the Environment.

Monitor and prevent potential unauthorized email traffic from IRS network.

What are the incoming connections to this Environment?

The IRS Internal Mail Relay sends copy of potential unauthorized email traffic to IBR email prevents Virtual Machines (VM)/ Internet Protocol Family (INET) Email Prevent VM that violates set IRM policies in the VMs.

What are the outgoing connections from this Environment?

Creation, deletion, and modification of policies to Prevent Virtual Servers, and blocking of potential unauthorized outbound emails from the prevent virtual servers to IRS internal mail relay.

What type of site is this?

Environment

What is the name of the Environment?

SPIIDE Data Loss Prevention (DLP) Data-In-Motion (DIM) Network Monitors

What is the sensitivity of the Environment?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the Environment.

Monitors unauthorized network traffic within the IRS network using Symantec Data Loss Prevention solution from Broadcom.

What are the incoming connections to this Environment?

Outbound network traffic, such as FTP, HTTP, and SNMP are sent from CISCO 3570x to the Network Monitor servers then to the enforce Management Console. All data are finally sent to the Enforce Management Console.

What are the outgoing connections from this Environment?

For network monitoring, the SDLP policies are sent to and enforced on HP DL 360 G7 servers, connected using Endace NIC. Then, these are connected to CISCO 3750x switches where the main network traffic traverses. The outgoing connections from the environment are for

managing policies on VMs, which monitor for specified network activities.