Date of Approval: **February 09, 2021**

PIA ID Number: **5828**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

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

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

SPIIDE DLP System, DLP, 3149

What is the approval date of the most recent PCLIA?

2/7/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Cybersecurity and Privacy Governance Board (CPGB) and Infrastructure Executive Steering Committee (ESC).

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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 Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) project is to implement a Data Loss Prevention (DLP) system, providing the IRS the ability to prevent the accidental loss or disclosure of taxpayer information, existing Personally Identifiable Information (PII) and Sensitive Agency Information (SAI). DLP is capable of monitoring email and internet communications for outgoing PII/SAI and prevent the loss or disclosure of unprotected PII/SAI information.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The SPIIDE DLP System is designed specifically to detect unencrypted SSNs or TINs that are being transmitted outside of the IRS Information Technology (IT) boundary via email or web interface. The SSNs and TINs detected are stored in the DLP System database which is encrypted using Federal Information Processing

Standard (FIPS) 140-2 approved algorithms. The SSNs/TINs can be taxpayer or IRS employee PII. The DLP System also has a blocking feature which will prevent detected SSNs/TINs from leaving the IRS IT boundary.

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

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. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. Safeguarding Personally Identifiable Information PCLIA requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

E-mail Address

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

Criminal History

Passport Number

Alien Number

Financial Account Numbers

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Procurement sensitive data Contract proposals, bids, etc.

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.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

No

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

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

The SPIIDE DLP System was purchased and deployed by the IRS to help prevent the illegal or unintentional dissemination of PII (specifically SSNs and TINs) outside the IRS. The system detects unencrypted SSNs/TINs 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 an SSN/TIN 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 the appropriate authority for further action. Event data access is limited to Event Responders only and cannot be accessed remotely.

How is the SBU/PII verified for accuracy, timeliness and completion?

The scope of the DLP solution is to monitor for Social Security Numbers (including Taxpayer Identification Numbers) 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 the 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 is important to verify that the numbers within an email are actually SSNs/TINs in order to execute appropriate incident response procedures.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

All IRS employees 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The DLP System is designed to detect inadvertent or possibly illegal dissemination of unencrypted SSNs/TINs leaving the IRS IT Boundary. The SSNs/TINs captured by the DLP System are stored in an encrypted database. The System is in place to prevent the dissemination of unencrypted taxpayer SSNs/TINs to unauthorized 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.

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 disciplinary 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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Write

Contractor System Administrators: Administrator

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 has 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

Data Loss Prevention SPIIDE (DLP) is scheduled (DAA-0058-2013-0010). All 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 35b, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

5/27/2020

Describe the system's audit trail.

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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

All test results were captured and are stored in the SPIIDE DLP SharePoint document depository.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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 functional testing. Strict accountability is achieved through the role-based access via OL5081. Functional testing has been conducted to ensure only the data required to identify the sender of unencrypted SSNs/TINs is collected by the system.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

10/2/2014

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: 100,000 to 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

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

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. Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigations (CI), etc.

Does computer matching occur?

Yes

Does your matching meet the Privacy Act definition of a matching program?

Yes

Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Yes

ACCOUNTING OF DISCLOSURES

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