Date of Approval: **October 18, 2019**

PIA ID Number: **4261**

SYSTEM DESCRIPTION

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

Streaming Data Monitoring Tool, SDMT

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?

Splunk Enterprise, Splunk, O&M, PIA 3912

What is the approval date of the most recent PCLIA?

7/19/2017

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

New Access by IRS employees or Members of the Public

Addition of Commercial Data or Sources

New Interagency Use

Internal Flow or Collection

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)

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 SDMT is to collect and generate audit records for security-related events. SDMT deploys Splunk Enterprise, on premises COTS tool to ingest and index data. Splunk assists Cybersecurity, Business Units, IRS projects, and Treasury Inspector General for Tax Administration (TIGTA) to detect unauthorized intrusions and privileged access abuse. Security audit information is defined as: A chronological record of user activities that is sufficient to enable the reconstruction, review, and examination of those activities A set of records that collectively provide evidence to support enforcement actions A set of auditable events that include all related user actions that lead up to a particular event. The audit trail record must convey these actions (i.e., user interface activities) in the record in a useful manner such that the auditable event and related actions can be reconstructed and presented in the context in which it happened. Standard Employee Identifiers (SEIDs) and Internet Protocol (IP) addresses are collected from security audit logs of various systems and are used to attribute security relevant system activity to the specific individual performing the action and the network host from which the action occurred. Splunk Enterprise collects and indexes any machine data from physical, virtual or cloud environments that can be used for security, compliance and fraud detection purpose, infrastructure and operational management purpose as well as for application delivery and quality assurance purpose.

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:

Legal/statutory basis (e.g. where collection is expressly required by statute)

Statistical and other research purposes

Law enforcement and intelligence purposes

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)

IRS has implemented technologies into the IRS enterprise that monitor the IRS applications and platforms to detect attacks, and indicators of potential attacks, and data loss prevention. Some of those technologies may capture social security numbers as they attempt to exit the IRS, or while being transported to other systems. Splunk will ingest those events.

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

Splunk indexes log events that may include sensitive information such as social security numbers which are forwarded by other IRS information monitoring systems. Splunk can be configured to mask social security numbers when indexing log events, but events in its raw form are required for NTIN (Negative Tax Identification Number) verification by other applications and hence can't be masked. Social security numbers, although processed by Splunk, can be anonymized through a regular expression and access control will be put in place to restrict the users allowing only ones to see PII data, who are privileged to fulfill the business requirements.

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

Phone Numbers

E-mail Address

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

Financial Account Numbers

Employment Information

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

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

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

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

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

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.

Personally Identifiable Information (PII), Taxpayer Information (TPI), Federal Tax Information (FTI), Standard Employee Identifier (SEIDs), Internet Protocol (IP) addresses, platform host names, and other similar data is collected by IRS technologies, and is used to validate and authenticate individuals trying to access IRS services. The information is required to ensure only valid and approved IRS taxpayers and Non-Filers may access IRS services. The following Internal Revenue Manuals (IRMs) provide requirements for external authentication of users to IRS systems, to include 10.5.1, 1.35.6, 10.8.1, and 10.8.2. It requires use of identity proofing elements such as taxpayer name, taxpayer address, taxpayer Social Security number and taxpayer date of birth and/or filing status. The other business use of the collected PII information is to conduct fraud analysis to identify and deter fraudulent usage of Electronic Authentication (eAuth) system by unauthorized users. The purpose of Splunk is to collect security audit information. Splunk assists Cybersecurity, Business Units, and Treasury Inspector General for Tax Administration (TIGTA) to detect unauthorized intrusions and privileged access abuse. Splunk would be used to alert business owners and the stakeholders mentioned when unauthorized access to any PII occurs, or an actionable event may need to be escalated to an incident.

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

All data collected by Splunk originates from other internal IRS applications and GSS (General Support System). These applications and GSS systems are responsible for ensuring SBU/PII is verified for accuracy, timeliness, and completeness. Splunk maintains the integrity of information stored after ingestion through a hashing mechanism to ensure no data is modified after ingestion. Splunk is a reporting tool and does not perform any action that modifies the data once it has been ingested and indexed. PII is submitted directly by the taxpayers and tax preparers. Once the user inputs their PII data, it gets validated against the IRS internal data source Integrated Customer Communications Environment (ICCE), validating they are who they say they are. If the information is not available for the users (Non-Filers), their PII data is validated against third party data service providers. Drop down menus and syntax requirements are enforced throughout the application to ensure the accuracy and completeness of data input. Once the PII is forwarded to Splunk, business owners can see any unauthorized access to their information and/or information systems in real-time.

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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 34.037 Audit Trail and Security Records

IRS 36.003 General Personnel and Payroll 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?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Totally Automated Personnel System (TAPS)
Current PCLIA: Yes
Approval Date: 10/5/2017
SA&A: Yes
ATO/IATO Date: 5/1/2017

System Name: GSS-24
Current PCLIA: Yes
Approval Date: 2/1/2017
SA&A: Yes
ATO/IATO Date: 2/9/2019

System Name: Security-1 (FSCT)
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 2/9/2017
System Name: KISAM

Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 5/22/2017

System Name: Electronic Authentication (eAuth)
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 11/2/2018

System Name: Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 3/6/2017
SA&A: Yes
ATO/IATO Date: 11/14/2016

System Name: Return Review Program (RRP)
Current PCLIA: Yes
Approval Date: 10/6/2017
SA&A: Yes
ATO/IATO Date: 6/23/2017

System Name: Prisoner Reporting Tool
Current PCLIA: Yes
Approval Date: 12/4/2017
SA&A: No
System Name: Coverage Data Repository (CDR)/Information Returns Database (IRDB)

Current PCLIA: Yes
Approval Date: 5/3/2018
SA&A: Yes
ATO/IATO Date: 5/31/2018

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 10/12/2018
SA&A: Yes
ATO/IATO Date: 1/12/2018

System Name: Business Masterfile Case Creation Non-Filer Identification Process (BMF_CCNIP)
Current PCLIA: Yes
Approval Date: 3/18/2018
SA&A: Yes
ATO/IATO Date: 8/24/2017

System Name: Branded Prescription Drugs (BPD)
Current PCLIA: Yes
Approval Date: 6/29/2018
SA&A: Yes
ATO/IATO Date: 11/2/2017

System Name: Counsel Automated Systems Environment Management Information System (CASEMIS)
Current PCLIA: Yes
Approval Date: 3/14/2018
SA&A: Yes
ATO/IATO Date: 5/10/2017

System Name: Compliance Data Environment (CDE)
Current PCLIA: Yes
Approval Date: 3/26/2017
SA&A: Yes
ATO/IATO Date: 5/10/2017

System Name: Correspondence Examination Automation Support (CEAS)
Current PCLIA: Yes
Approval Date: 2/14/2018
SA&A: Yes
ATO/IATO Date: 12/18/2017

System Name: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 12/17/2017
SA&A: Yes
ATO/IATO Date: 4/3/2017

System Name: Electronic Federal Payment Posting System (EFPPS)
Current PCLIA: Yes
Approval Date: 5/4/2018
SA&A: Yes
ATO/IATO Date: 1/18/2018

System Name: Embedded Quality Review System - Campus (EQRSC)
Current PCLIA: Yes
Approval Date: 12/8/2016
SA&A: Yes
ATO/IATO Date: 3/30/2017

System Name: Embedded Quality Review System - Field (EQRSF)
Current PCLIA: Yes
Approval Date: 2/25/2019
SA&A: Yes
ATO/IATO Date: 3/28/2017

System Name: Examination Returns Control System (ERCS)
Current PCLIA: Yes
Approval Date: 2/17/2017
SA&A: Yes
ATO/IATO Date: 3/13/2017

System Name: Corporate Authoritative Directory Service (CADS)
Current PCLIA: Yes
Approval Date: 2/6/2017
SA&A: Yes
ATO/IATO Date: 9/11/2017

System Name: Return Integrity and Compliance Services (RICS)
Current PCLIA: Yes
Approval Date: 3/31/2017
SA&A: Yes
ATO/IATO Date: 9/11/2017

System Name: Information Returns Master File Processing (IRMF)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 2/5/2018

System Name: Automated Lien System - ENTITY Case Management (ALS ENTITY)
Current PCLIA: Yes
Approval Date: 11/16/2016
SA&A: Yes
ATO/IATO Date: 10/10/2017

System Name: Automated Lien System - ENTITY Case Management (ALS ENTITY)
Current PCLIA: Yes
Approval Date: 11/16/2016
SA&A: Yes
ATO/IATO Date: 10/10/2017

System Name: Automated Manual Assessments (AMA)
Current PCLIA: Yes
Approval Date: 5/3/2018
SA&A: Yes
ATO/IATO Date: 1/1/2018

System Name: Account Management System (AMS)
Current PCLIA: Yes
Approval Date: 9/26/2017
SA&A: Yes
ATO/IATO Date: 4/3/2017

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 8/28/2017
SA&A: Yes
ATO/IATO Date: 1/17/2018

System Name: Foreign Account Tax Compliance Act (FATCA)
Current PCLIA: Yes
Approval Date: 7/18/2017
SA&A: Yes
ATO/IATO Date: 9/30/2019

System Name: Federal Student Aid IRS Datashare (FSA-D)
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 9/4/2018

System Name: First Time Home Buyers Credit (FTHBC)
Current PCLIA: Yes
Approval Date: 3/11/2019
SA&A: Yes
ATO/IATO Date: 9/2/2018

System Name: Get Transcript (GETTRANS)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 3/12/2019

System Name: Health Coverage Tax Credit (HCTC)
Current PCLIA: Yes
Approval Date: 3/21/2019
SA&A: Yes
ATO/IATO Date: 12/27/2017

System Name: Enterprise level web-based data Tracking (eTRAK)
Current PCLIA: Yes
Approval Date: 3/11/2019
SA&A: Yes
ATO/IATO Date: 1/18/2018

System Name: Excise Files Information Retrieval System (EXFIRS)
Current PCLIA: Yes
Approval Date: 1/13/2017
SA&A: Yes
ATO/IATO Date: 4/19/2017

System Name: Excise Summary Terminal Activity Reporting System (ExSTARS)
Current PCLIA: Yes
Approval Date: 1/13/2017
SA&A: Yes
ATO/IATO Date: 4/19/2017

System Name: Remittance Strategy for Paper Check Conversion (RSPCC)
Current PCLIA: Yes
Approval Date: 9/23/2016
SA&A: Yes
ATO/IATO Date: 1/4/2018

System Name: Remittance Transaction Research (RTR)
Current PCLIA: Yes
Approval Date: 5/3/2018
SA&A: Yes
ATO/IATO Date: 1/4/2018

System Name: Service Wide Employment Tax Research System (SWETRS)
Current PCLIA: Yes
Approval Date: 2/12/2019
SA&A: Yes
ATO/IATO Date: 12/20/2017

System Name: Transcript Delivery System (TDS)
Current PCLIA: Yes
Approval Date: 11/3/2015
SA&A: Yes
ATO/IATO Date: 3/22/2017

System Name: Tax Litigation Counsel Automated Tracking System (TLCATS)
Current PCLIA: Yes
Approval Date: 5/9/2019
SA&A: Yes
ATO/IATO Date: 11/20/2017

System Name: TIN Matching (TM)
Current PCLIA: Yes
Approval Date: 8/7/2019
SA&A: Yes
ATO/IATO Date: 3/22/2017

System Name: Tax Identification Number (PTIN) System (TPPS)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 3/29/2017

System Name: Web-Based Employee Technical Time System (WEBETS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 12/5/2016

System Name: Withholding Compliance System (WHCS)
Current PCLIA: Yes
Approval Date: 3/29/2018
SA&A: Yes
ATO/IATO Date: 8/24/2017

System Name: Where's My Amended Return (WMAR)
Current PCLIA: Yes
Approval Date: 5/29/2019
SA&A: No

System Name: Automated Enrollment (AE)
Current PCLIA: Yes
Approval Date: 2/23/2016
SA&A: Yes
ATO/IATO Date: 12/21/2017

System Name: Automated Freedom of Information Act (AFOIA)
Current PCLIA: Yes
Approval Date: 11/3/2017
SA&A: Yes
ATO/IATO Date: 1/18/2018

System Name: Big Data Analytics (BDA)
Current PCLIA: Yes
Approval Date: 11/3/2017
SA&A: Yes
ATO/IATO Date: 12/15/2016

System Name: Internet Refund-Fact of Filing (IRFOF)
Current PCLIA: Yes
Approval Date: 3/30/2016
SA&A: No

System Name: Taxpayer Identification Number - Real Time System (ITIN RTS)
Current PCLIA: Yes
Approval Date: 2/13/2018
SA&A: Yes
ATO/IATO Date: 1/4/2018

System Name: Modernized E File (MEF)
Current PCLIA: Yes
Approval Date: 2/20/2019
SA&A: Yes
ATO/IATO Date: 12/21/2017

System Name: Modernized Internet Employer Identification Number (MODIEIN)
Current PCLIA: Yes
Approval Date: 3/30/2016
SA&A: No

System Name: Order a Transcript (OAT)
Current PCLIA: Yes
Approval Date: 4/28/2019
SA&A: Yes
ATO/IATO Date: 5/1/2019

System Name: Online Account (OLA)
Current PCLIA: Yes
Approval Date: 12/23/2016
SA&A: Yes
ATO/IATO Date: 1/22/2017

System Name: GSS-30
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 6/2/2016

System Name: GSS-42
Current PCLIA: Yes
Approval Date: 4/17/2019
SA&A: Yes

ATO/IATO Date: 3/3/2017
System Name: GSS-17
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 2/9/2017

System Name: ACA Information Returns (AIR)
Current PCLIA: Yes
Approval Date: 12/21/2018
SA&A: Yes
ATO/IATO Date: 5/31/2018

System Name: TIN Validation - Enterprise Common Service (TIN-ECS)
Current PCLIA: Yes
Approval Date: 2/5/2019
SA&A: No

System Name: Security-1 (SPIIDE)
Current PCLIA: Yes
Approval Date: 3/31/2015
SA&A: Yes
ATO/IATO Date: 3/14/2016

System Name: GSS-26
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 1/26/2017

System Name: GSS-38
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 5/17/2017

System Name: Security-1 (SAAS)
Current PCLIA: Yes
Approval Date: 4/13/2018
SA&A: Yes
ATO/IATO Date: 3/14/2016

System Name: External Services Authorization Management (ESAM)
Current PCLIA: Yes
Approval Date: 11/3/2015
SA&A: Yes
ATO/IATO Date: 3/22/2017

System Name: Enterprise web-based suite of Services (eServices)
Current PCLIA: Yes
Approval Date: 4/20/2018
SA&A: Yes
ATO/IATO Date: 3/22/2017

System Name: International Compliance Management Model FATCA International Returns (ICMM FIR)
Current PCLIA: Yes
Approval Date: 1/30/2018
SA&A: Yes
ATO/IATO Date: 7/18/2017

System Name: Integrated Financial System (IFS)
Current PCLIA: Yes
Approval Date: 4/27/2017
SA&A: Yes
ATO/IATO Date: 10/13/2017

System Name: Issue Management System (IMS)
Current PCLIA: Yes
Approval Date: 9/3/2019
SA&A: Yes
ATO/IATO Date: 5/7/2017

System Name: Online Payment Agreement (OPA)
Current PCLIA: Yes
Approval Date: 3/13/2019
SA&A: Yes
ATO/IATO Date: 6/27/2018

System Name: Reporting Compliance Case Management System (RCCMS)
Current PCLIA: Yes
Approval Date: 10/18/2017
SA&A: Yes
ATO/IATO Date: 10/27/2017

System Name: Lead and Case Analytics Project Charter (LCA)
Current PCLIA: Yes
Approval Date: 6/30/2018
SA&A: Yes
ATO/IATO Date: 2/14/2018

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

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1095-A Form Name: Health Insurance Marketplace Statement

Form Number: 1095-B Form Name: Health Coverage

Form Number: 1095-C Form Name: Employer-Provided Health Insurance Offer and Coverage

Form Number: 1094-C Form Name: Transmittal of Employer-Provided Health Insurance Offer and Coverage Information Returns

Form Number: 1094-B Form Name: Transmittal of Health Coverage Information Returns

Form Number: SF-85 Form Name: Questionnaire for Non-Sensitive Positions

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

Yes

Please identify the form number and name:

Form Number: SF-85 Form Name: Questionnaire for Non-Sensitive Positions

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Tax Return Database (TRDB)
Current PCLIA: Yes
Approval Date: 10/30/2018
SA&A: No

System Name: Enterprise Directory Agent (EDA)
Current PCLIA: Yes
Approval Date: 3/3/2017
SA&A: No

System Name: Individual Return Master File (IRMF)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 11/18/2016

Identify the authority

5 U.S.C 301, 1302, 2951, 4118, 4308 and 4506 18 U.S.C. 1030 (a)(2)(B) 26 U.S.C. 7801 Executive Orders 9397 and 10561.

For what purpose?

To maintain records of individual and business tax returns, return transactions and authorized taxpayers. To identify and track any unauthorized accesses to sensitive but classified information and potential breaches or unauthorized disclosures of such information. To administer personnel and payroll programs.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

Users accessing the IRS LAN (Local Area Network) and other systems are notified that their activity may be monitored through the following warning banner that is displayed prior to granting access: ****THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!**** Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subjected to criminal and civil penalties. All IRS systems are required to display this banner upon system login.

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

No

Why not?

Splunk only collects information from other IRS systems.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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 Only

Managers: Read Only

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

Individuals must submit an Online 5081 request for access. Access approval must be granted by the user's federal manager and approver groups prior to access being granted.

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.

The National Archives and Records Administration (NARA) approved the destruction of Splunk audit data when 7 years old (Job No. N1-58-10-22, approved 4/5/2011). Splunk retention requirements are published under IRS Document 12990, Records Control Schedule 19 for Martinsburg Computing Center, item 88 for Security Auditing and Analysis System (SAAS). Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records.

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?

3/28/2017

Describe the system's audit trail.

The following events are recorded in the Splunk audit trail: - Logon/logoff (Captured in GSS-17 logs) - Creation/modification of user groups (Captured in GSS-17 logs) - All system administrator (SA) actions + System configuration settings + Creation/Modification/Deletion of data inputs - All user actions + Creation/Modification/Deletion of Knowledge Objects (Dashboards, Visualizations, Searches) + Search execution Clearing of the audit log file Startup and shut down of audit functions Change of file or user permissions or privileges (suid/guid, chown, su, etc.) (captured in GSS-42 logs) . Once approved, Splunk will process PII, SBU, and other taxpayer-related information from other systems. This data will be indexed, reviewed, analyzed, and reported Splunk stakeholders. UserID, Usertype, System, EventType, EventID, TaxfilerTIN, SessionID, ScrAddr, ReturnCode, ErrorMsg, TimeStamp, VarData(Payload), TaxPeriod, MFTCode, ReturnType, and TaxfilerTINType.

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)?

Security Controls Assessment Testing has been completed. Authority to Operate (ATO) signed 3/28/17.

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?

Security Controls Assessment Testing has been completed. Authorization to Operate (ATO) signed 3/28/17.

SBU DATA USE

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

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: More than 100,000

Contractors: More than 10,000

Members of the Public: More than 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.

Splunk will collect and store security audit records of IRS employees and contractors accessing IRS systems and IRS facilities.

Does computer matching occur?

No

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