Date of Approval: 09/24/2025
Questionnaire Number: 2457

Basic Information/Executive Summary

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

CI-1 | Splunk

Acronym:

CI-1 | Splunk

Business Unit

Criminal Investigation

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.

Criminal Investigation (CI) utilizes Splunk Enterprise to meet the Continuous Diagnostic and Mitigation (CDM) program requirements. Splunk collects and indexes real-time log data from CI log sources into a searchable repository from which graphs, reports, alerts, dashboards, and visualizations can be generated. The legal requirement for this solution is OMB M-21-31. This Splunk Enterprise instance resides on-premises, within the Criminal Investigation System Domain (CI-1) authorization boundary. CI implemented Splunk in 2017 and will continue to use Splunk until the Internal Revenue Service decides otherwise due to licensing. This instance of Splunk is separate to the Streaming Data Monitoring Tool (SDMT) instance used by the Civil components of the Internal Revenue Service.

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).

Splunk is a repository tool that doesn't have any sensitive data of its own that it creates. But it stores sensitive data that may be generated in the logs of other tools. That data for all SSN/TIN is masked when ingested and only utilized for audit purposes. Data is then stored and will be archived for up to 20 years depending on the data requirements.

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

Criminal Investigation Information
Email Address
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
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).

Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
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

1.1 What is the name of the Business Unit (BU) or Agency initiative?

Criminal Investigation System Domain

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)

Tier 3

4 Is this a new system?

No

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

No

4.11 What is the previous PCLIA number?

No

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

CI-1 | Splunk

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

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

Yes

5.1 Identify the parent system's approved PCLIA number.

Previously approved PCLIA is 7593. CI-1's new PCLIA is currently going through the approval process.

5.2 Identify the parent system's name as previously approved.

Criminal Investigation System Domain (CI-1)

7 Is this a change resulting from the OneSDLC process?

No

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

Criminal Investigation Governance Board, Sustaining Ops Executive Steering Committee

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.

211298

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.

There is no disclosure outside of the IRS.

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)

There is not a process for this. The system uses information provided from the IT assets that are connected to the network.

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.)

Only Splunk Administrators have access to the PII in the system.

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 banners included at initial logon.

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".

Not applicable

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

Access to SBU/PII is determined by the user having a valid Business Entitlement Access Request System (BEARS) authorization. There are multiple approvers for a BEARs entitlement.

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

No

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

There are no identified privacy and civil liberties risks related to privacy controls at this time.

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.

CI-1 Splunk's audit trail is contained within its own index within the system. The system events generated by the Splunk platform are contained in an index and searchable. The Splunk ESAT worksheet will be uploaded as part of the evidence package.

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

No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Qualys
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
CI LIMS FORAY
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarders

Interface Type
IRS Systems, file, or database
Agency Name
CI-1 | BigFix
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarder

Interface Type
IRS Systems, file, or database
Agency Name
CI CIMIS
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database

Agency Name
CI-1 | PUMAS
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarder

Interface Type
IRS Systems, file, or database
Agency Name
CI Silo
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Criminal Investigation System Domain (CI-1)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarders

Interface Type
IRS Systems, file, or database
Agency Name
CI LCA
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarder

Interface Type
IRS Systems, file, or database
Agency Name
CI-1 | Splunk

Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Internal Splunk logs are held within the Splunk instance for audit requirements

Interface Type
IRS Systems, file, or database
Agency Name
CI NIMBUS
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk Forwarder

Interface Type
IRS Systems, file, or database
Agency Name
CI Box
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk forwarder

Interface Type
IRS Systems, file, or database
Agency Name
CI-1 | Forescout
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Splunk Forwarder

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.

To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

SORN Number & Name

IRS 42.008 - Audit Information Management System

Describe the IRS use and relevance of this SORN.

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted. To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

036

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Cybersecurity logging records. For additional information about these records, see OMB Memo M-21-31. Note: The requirements in OMB Memo M-21-31 do not apply to national security systems. Agencies may use this GRS for national security systems or submit an agency-specific schedule. Cybersecurity event logs. Logs required by OMB Memo M-21-31 to capture data used in the detection, investigation, and remediation of cyber threats. Legal citation: OMB Memo M-21-31 Not media neutral. Applies to electronic records only.

What is the disposition schedule?

Temporary. Destroy when 30 months old. Longer retention is authorized for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

030

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: • user profiles • log-in files • password files • audit trail files and extracts • system usage files • cost-back files used to assess charges for system use

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.

What is the disposition schedule?

Temporary. Destroy when business use ceases.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

31

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: • user profiles • log-in files • password files • audit trail files and extracts • system usage files • cost-back files used to assess charges for system use

Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.1 General Technology Management Records

What is the GRS/RCS Item Number?

020

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Information Technology Operations and Maintenance records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.

What is the disposition schedule?

Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Data Locations

What type of site is this?

System

What is the name of the System?

CI-1 | Splunk

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

Splunk provides centralized log management, search, correlation, alerting, dashboards, and reporting to support security operations, incident response, audit/forensics, and compliance. It ingests machine data (e.g., OS logs, application logs, network telemetry, cloud audit trails) to detect, investigate, and report on security and privacy incidents.

What are the incoming connections to this System?

Information flows into Splunk from many parts of the enterprise. Servers and devices automatically send their log data to Splunk. In some cases, applications or cloud services send activity data directly into Splunk through secure connections. Authorized staff may also log into Splunk through a web interface to search data or view dashboards. In simple terms, Splunk “listens” for log information from the organization’s technology environment so it can be analyzed in one place.

What are the outgoing connections from this System?

Splunk also communicates outward when necessary to share findings or retrieve supporting data. For example, it can send alerts by email. Splunk may also reach out to approved external services to download updated threat intelligence or to pull in vulnerability information. Additionally, backups of Splunk data are securely sent to agency-approved storage. All these outgoing connections are limited, monitored, and used only to support security operations and compliance reporting.