Date of Approval: 04/08/2025
Questionnaire Number: 2169

Basic Information/Executive Summary

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

Criminal Investigation - Tactical Law Enforcement Operational Network

Acronym:

TaLON

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.

The Criminal Investigation - Tactical Law Enforcement Operational Network (TaLON) is a common technology network platform to rapidly field powerful and relevant law enforcement technology, securely, to our agents and investigators, to mitigate the risks of law enforcement activities from the core IRS network. The network would allow dark web reconnaissance, A cryptocurrency intelligence gathering, social media and open-source intelligence operations, along with task force access to off network resources. The agent will be able to log into TaLON using the onsite designated TaLON desktop or assigned Chromebook via an OKTA account. Only the agent will have access to any information gathered. No information is stored within TaLON.

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).

1.Inception (Log Generation) TaLON Audit logs are generated when events occur in each system categories. This happens at various levels, including Utility Computers, Cloud Tools/applications, and Network devices. These logs often capture PII Data, such as: Authentication Details - Username, IP addresses, login timestamps, authentication methods. User Activity - Logins, file access, data modifications, administrative actions. Error Messages - Failed login attempts, system errors, security warnings. The logging mechanism collects data through Universal Forwarders or Application Programming Interface (API) calls (e.g., Syslog, Windows Event Viewer, Service as a Service (SaaS) tools) and stores it in Splunk Cloud.
2. Transmission and Storage Secure Transmission: Logs are sent to Splunk via encrypted channels (e.g., Transaction Control Language (TLS), Virtual Private Network (VPN) tunnels). Storage in Splunk: Logs are indexed and stored in Splunk's distributed architecture, ensuring redundancy and security. Access Control: Role-Based Access Control (RBAC) in Splunk restricts log access to authorized personnel. Retention Policies: Logs are retained based on organizational policies (2 year) and compliance requirements.
3. Processing and Analysis Stored logs are analyzed to detect security incidents, ensure compliance, and troubleshoot system issues. Security Monitoring - Splunk analyzes logs for anomalies (e.g., failed login attempts, unauthorized access). Compliance Audits - Logs are reviewed for regulatory compliance Masking and Redaction - Splunk applies field masking to hide sensitive data in logs before processing (e.g., PII, credit card numbers)
4. Destruction and Disposal When logs reach the end of their retention period, they must be securely destroyed to prevent unauthorized access. Log Purging - Automated scripts delete old logs based on retention policies.

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

Internet Protocol Address (IP Address)
Name
Other

Please explain the other type(s) of PII that this project uses.

Username

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
Information by CI for certain money laundering cases - 18 USC

Product Information (Questions)

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

1.1 What is the name of the Business Unit (BU) or Agency initiative?
Criminal Investigations (CI) - Business Systems Development (BSD)

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?
1

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
No

4.2 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.)
The PCLIA was not completed originally when the system was setup.

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.
Tech Insertion is being utilized. TaLON is going through the security assessment.

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.
Configuration Control Board

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.

No

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?

Yes

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?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Tenable - Package ID FR1814276801 - 09/22/2021; Okta - Package ID F1512167750 - 04/26/2017; Google Workspace - Package ID F1206081364 - 10/28/2021; CrowdStrike - Package ID FR1807853629 - 09/19/2018; AWS - Package ID F1603047866 - 06/21/2016; Splunk - Package ID F1607197917 - 10/11/2019

12.2 Does the CSP allow auditing?

Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate

13 Does this system/application interact with the public?

No

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

No

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

This information used for investigative purposes.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

This information collected is used for investigative purposes. The individual being investigated may not be aware of the investigation until the agent has gathered enough information to build the case.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

This information collected is used for investigative purposes. The individual being investigated may not be aware of the investigation until the agent has gathered enough information to build the case.

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

Not Applicable

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.)

Roles: User - Read Only; Manager - Read and Write; System Administrator - Administrator and Developer - Read Only

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.

The IRS has established internal processes, procedures, and administrative controls to ensure compliance with the Privacy Act of 1974, as amended (5 United States Code 552a), Appendix 1 to OMB Circular A-130, and Internal Revenue Code 6103 ("Confidentiality and disclosure of returns and return information").

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".

Not Applicable

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".

Not Applicable

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?

The IRS is required to instill a SBU Data Use process to monitor, regulate and ensure the security and privacy measures are in place before SBU Data is approved to be used in a non-production environment.

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

No

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.

No

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

Deactivation and deletion requests are approved by authorized personnel and logged in Splunk’s event indexes, providing a detailed audit trail. All incident responses are logged in Splunk with detailed metadata, providing a complete audit trail for compliance purposes. CI-TaLON collects and retains audit logs that are produced on the local systems and off-loaded into Splunk for data retention.

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

No

Interfaces

Interface Type

IRS or Treasury Contractor

Agency Name

Okta

Incoming/Outgoing

Incoming (Receiving)

Transfer Method
Other
Other Transfer Method
Provides centralized identity and access management capabilities to customers who want to manage access across any application or device, whether on-premises or in the cloud.

Interface Type
IRS or Treasury Contractor
Agency Name
Amazon Web Services Platform (AWS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
This provides true cloud architecture, on-demand elasticity, seamless application migration, cloud-native integration, and business continuity and disaster recovery.

Interface Type
IRS or Treasury Contractor
Agency Name
Splunk
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
It offers a cloud-based service that allows users to search, analyze, and visualize machine-generated data from various sources, including websites, applications, sensors, and devices.

Interface Type
IRS or Treasury Contractor
Agency Name
CrowdStrike
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Enables customers to identify unknown malware, detect zero-day threats, identify advanced adversaries, and prevent damage from targeted attacks in real-time.

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 46.002 - Criminal Investigation Management Information System and Case Files

Describe the IRS use and relevance of this SORN.

The IRS CI agents abide by the details outlined in the SORN to complete their investigations.

Records Retention

What is the Record Schedule System?

Non-Record

Data Locations

What type of site is this?

System

What is the name of the System?

Splunk

Please provide a brief description of the System.

Splunk Cloud provides operational intelligence capabilities to organizations around the world. It offers a cloud-based service that allows users to search, analyze, and visualize machine-generated data from various sources, including websites, applications, sensors, and devices. The platform is designed to handle large volumes of data, providing real-time insights, and enabling organizations to make data-driven decisions.

What are the incoming connections to this System?

Logs are sent to Splunk via encrypted channels (e.g., TLS, VPN tunnels).