Date of Approval: 09/12/2025
Questionnaire Number: 2338

Basic Information/Executive Summary

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

Host Based Intrusion Detection System - Endpoint Detection & Response

Acronym:

HIDS-EDR

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.

Endpoint Detection & Response is an agent-based software application that uses intelligence information to locate emerging malicious threat activity on Internal Revenue Service workstations and servers and providing a playback of endpoint activity around those threats for Cyber incident investigations and reporting. It will provide the Computer Security Incident Reporting Center (CSIRC) incident handlers a full on-host snapshot of potentially malicious, malformed, or misused data to the CSIRC security information event management (SIEM).

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).

This tool is used to collect key endpoint data (Domain Name System [XXXXXX] requests, Uniform Resource Identifier [XXXXX] accessed, registry key changes, file system changes, running processes, etc.) surrounding security events that occur on a host which will provide the IRS Computer Security Incident Response Center (CSIRC) with the capability to collect host event data for framing the attack structure of related security events. The forensics tool data that must be collected will be used to frame how a security event was triggered; thus, providing information as to the overall risk the threat presents to the enterprise and assist CSIRC in creating a mitigation of the threat moving forward. Any SBU/PII data that is unintendedly collected as a part of the system data provided will not be used in any capacity than to provide a means of framing the overall risk of the security event to the enterprise. We do not have individual records in the system. To clarify, the nature of the product is an endpoint security product. We collect data based on the event triggers. Any potential SBU/PII data collected would be a part of security investigation. The data collected is just a byproduct of the security investigation.

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

Address
Email Address
Internet Protocol Address (IP Address)
Name
Other
Standard Employee Identifier (SEID)
Telephone Numbers

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

Tax Account Information and Date of Birth

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC

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)
4

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?
7084

4.12 What is the previous PCLIA title (system name)?
Host Based Intrusion Detection System - Endpoint D, HIDS-EDR

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.)
Prior PCLIA is expiring

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.
This system is in operations support phase. We do not have to do One SDLC. We completed our ELC process in 2020.

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.
Cybersecurity and Privacy (CP)

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.

The system does not disclose any PII to any third party outside of the IRS. Therefore, we do not need a process in place for this.

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)

This is an endpoint detection agent that is on all workstation to monitor threat intrusion therefore due process does not apply.

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

Yes

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

No

15.2 What PII/SBU data does the subcontractor(s) have access to?

No subcontractors are on this contract. The contractor [XX] has access to the system as part of the contract which is Operations & Maintenance.

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.)

The IRS currently uses the Admin, Analyst, API Admin, and API Analyst roles. The admin role is what the IRS and its contractors most privileged roles are and

are used most often. These roles allow changes to the Policies, rules, and host sets that manage the framework of the IRS enterprise. This role also allows the users to enter "configuration mode" in the command line interface (CLI) which allows the user to manage the appliance itself from the authentication of certificates to the welcome message displayed when first connecting to the appliance interface. The Analyst role is not used as much as it provides much less privileges mainly only allowing a few changes to host sets and visibility into rules and their data. The API roles are much the same as their non-API counterparts, but they allow API calls though scripts and pulls using these accounts. The difference being is that they are only have access during data pulls and when scripts are active. The IRS and contractors use these roles to perform these data pulls for reports and sending data to Splunk. The roles tied to the employees PII is their admin role and they sign in with this role if using their PIV card to sign in.

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 system does not interact with the public. This is an endpoint detection on the laptop.

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".

120000 endpoints, it's on all endpoint.

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 5000

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 HIDS-EDR system utilizes the standard IRS on-line access application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. Users are assigned to specific modules of the application and

specific roles within the modules and accounts follow the principle of least privilege which provide them the least amount of access to PII/SBU data that is required to perform their business function after receiving appropriate approval

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 privacy and/or civil liberties risk.

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.

The audit trail is provided by the Enterprise Security Audit Trail (ESAT) team.

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

SPLUNK

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure Data Transfer (SDT)

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 is cited to routine uses and for the purposes of identifying and tracking 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.

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Information systems security records
What is the GRS/RCS Item Number?
3.2/020
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
Computer security incident handling, reporting and follow-up records. A computer incident within the Federal Government as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 2, (August 2012) is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
What is the disposition schedule?
Temporary. Destroy 3 year(s) after all necessary follow-up actions have been completed, 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?
SPLUNK
What is the sensitivity of the System?
Sensitive But Unclassified (SBU)
Please provide a brief description of the System.
SPLUNK is an appliance-based product, which performs and stores database discovery and database vulnerability scans to meet Internal Revenue Manual and Federal Information Security Management Act (FISMA) requirements.
What are the incoming connections to this System?
This is a backend system to system transfer of data.