

Date of Approval: 08/04/2026
Questionnaire Number: 3051

Basic Information/Executive Summary

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

Compliance Optimization Monitoring Platform for Assessing Selections & Safeguards

Acronym:

COMPASS

Business Unit

Information Technology

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 COMPASS application is a mission critical, cloud-native, stand-alone automated system designed to maximize fraud detection at the time tax returns are filed to eliminate the issuance of questionable refunds. COMPASS detects reliable indicators of taxpayer fraud, keying highly focused investigations prior to the issuance of the refund, which has resulted in millions of dollars saved by stopping the issuance of fraudulent and erroneous refunds. COMPASS application uses mission data stored in IRS Enterprise Data Platform for case selection and integrates with Palantir-based Secure Tax Reporting and Insights Data Ecosystem (STRIDE) boundary. The Cloud Security Boundary External Partner Zone is used to connect EDP (cloud) to the Palantir Cloud. The only users of the COMPASS system are Criminal Investigation and Taxpayer Services employees. The Palantir

cloud infrastructure is managed by Palantir employees. The COMPASS application has replaced the on-premise Internal Revenue Services (IRS) system, “Enterprise Fraud Detection System” (EFDS). This application was designed to maximize fraud detection at the time tax returns were filed. This functionality eliminated the issuance of questionable and potentially fraudulent refunds. ess.

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).

The COMPASS project utilizes sensitive data (SBU/PII), including Social Security Numbers (SSNs), from inception to destruction in a manner strictly aligned with IRS mission requirements and federal privacy regulations. At inception, COMPASS receives SBU/PII from various sources of internal IRS systems, leveraging SSNs as the unique identifier necessary for cross-system fraud detection and tax administration, as authorized by Internal Revenue Code Section 6109. The data is limited to what is relevant for preventing lost revenue due to fraudulent tax returns, and its use is further restricted by enterprise access controls and compliance requirements. Upon receipt, COMPASS performs data health and integrity checks - to ensure accuracy, timeliness, and completeness, with discrepancies prompting retransmission from upstream sources. COMPASS processes data from the Enterprise Data Platform (EDP) and returns the data to EDP after processing. COMPASS does not retain any PII data.

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

Address

Device Identification (ID)

Document Locator Number (DLN)

Employer Identification Number

Family Members

Federal Tax Information (FTI)

Internet Protocol Address (IP Address)

Preparer Taxpayer Identification Number (PTIN)

Standard Employee Identifier (SEID)

Telephone Numbers

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

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

Product Information (Questions)

1 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

2 What Tier designation has been applied to your system? (Number)

3

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

No

4 Has a Privacy and Civil Liberties Impact Assessment (PCLIA) previously been completed for this system or application?

No

4.1 Was this system or application previously covered under a parent system and is now submitting its first PCLIA?

No

4.2 Is the system or application currently in production or operational use without a previously completed PCLIA?

No

5 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.

Not Applicable

6 Is this a change resulting from the OneSDLC process?

No

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

Strategic Development (SD) - this was the previous steering committee. This might change because of the reorganization that has occurred.

8 Is this System listed on As-Built-Architecture (ABA)? If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

Yes

8.1 What is the ABA ID?

212014

9 Does this system disclose any PII to any third party outside the IRS?

No

10 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

11 Does this system use cloud computing?

Yes

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

Palantir Federal Cloud Service, FR2434554673, 11/19/2024

11.2 Does the CSP allow auditing?

Yes

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

IRS

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

Moderate

12 Does this system/application interact with the public?

No

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

Notice, consent, and due process are provided through the instructions accompanying the tax forms and other tax administration forms completed and submitted by the taxpayer, and pursuant to 5 U.S.C.

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

Yes

14.1 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

14.2 What PII/SBU data does the contractor(s) and/or subcontractor(s) have access to?

Address, Device Identification (ID), Document Locator Number (DLN),
Employer Identification Number, Family Members, Federal Tax Information
(FTI), Internet Protocol Address (IP Address), Preparer Taxpayer Identification
Number (PTIN), Standard Employee Identifier (SEID), Telephone Numbers

15 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.)

IRS Employees? Yes/No Access Level
(Users, Yes, Read/Write)
(Managers, Yes, Read/Write)
(Sys. Administrators, Yes, Read/Write/Admin)
(Developers, Yes, Read/Write/Admin)

Contractor Employees? Yes/No Access Level Background Invest. Level
(Contractor Users, No)
(Contractor Managers, Yes, Read/Write, Public Trust (MBI))
(Contractor Sys. Admin, Yes, Read/Write/Admin, Public Trust (MBI))
(Contractor Developers, Yes, Read/Write /Admin, Public Trust (MBI))

16 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.

Welcome to the Palantir Platform. 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. Unauthorized use of this system is prohibited and
subject to criminal and civil penalties, including all penalties applicable to willful
unauthorized access (UNAX) or inspection of taxpayer records (under 18 U.S.C.
1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431). IRS Intranet Privacy Policy and
Privacy Act Statement.

17 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

18 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

19 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".
More than 1,000,000

20 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".
N/A

21 How is access to SBU/PII determined and by whom?
The COMPASS system utilizes the standard IRS on-line access application (BEARS) 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 with the least amount of access to PII/SBU data that is required to perform their business function after receiving appropriate approval.

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

23 Explain any privacy and civil liberties risks related to privacy controls.
There are no known privacy risk to the system at the moment.

24 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

25 Describe this system's audit trail in detail. Provide supporting documents.
ESAT Splunk is connected to the Palantir platform that pulls any logs required for auditing. Audit Trails include all user interface activities; the SBU elements attributed to the auditable event are the events success/fail status, date stamp, user's SEID, and an IP address. COMPASS users do not have access to Splunk auditing information and can only access system logs for required for troubleshooting. Access to system logs is further controlled by the Splunk BEARS entitlement. All user actions are recorded and timestamped within the Palantir logs and can be accessed for any specific audit requests. This data is retained for a period that is equal to the retention period of each record. Logs

collect all user actions with timestamps, which includes employee log-in information.

26 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

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Enterprise Data Platform (EDP)

Incoming/Outgoing

Both

Transfer Method

Amazon Web Services Platform (AWS)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

Individuals who file business tax and information returns; individuals who file other information filings; and individuals operating under powers of attorney for these businesses. Tax records for each applicable tax year or period, including employment tax returns, partnership returns, excise tax returns, retirement and employee plan returns, wagering returns, estate tax returns; information returns.

SORN Number & Name

IRS 22.061 - Information Return Master File

Describe the IRS use and relevance of this SORN.

Information Returns - Individual payors and payees of various types of income for which information reporting is required (e.g., wages, dividends, interest, etc.) To administer tax accounts related to the filing of information returns.

SORN Number & Name

IRS 46.050 - Automated Information Analysis System

Describe the IRS use and relevance of this SORN.

To maintain, analyze, and process records and information that may identify patterns of financial transactions indicative of criminal and/or civil noncompliance with tax, money laundering, Bank Secrecy Act, and other financial laws and regulations delegated to CI for investigation or enforcement, and that identifies or may identify the individuals connected to such activity. To establish linkages between fraudulent transactions or other activities, and the individuals involved in such actions, that may be used to further investigate such activity and to perfect filters that identify information pertaining to such activity.

SORN Number & Name

IRS 42.021 - Compliance Programs and Projects Files

Describe the IRS use and relevance of this SORN.

To track information relating to special programs and projects to identify non-compliance schemes and to select individuals involved in such schemes for enforcement actions.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

Tax records for each applicable tax period or year.

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 46.002 - Criminal Investigation Management Information System and Case Files

Describe the IRS use and relevance of this SORN.

Records pertaining to possible violations of laws under the enforcement jurisdiction of the IRS, received by the IRS from other sources or developed during investigative activities, that identify or may identify criminal or civil nonconformance with Federal tax laws and other Federal laws delegated to CI for investigation or enforcement; information arising from investigative activities conducted by CI in conjunction with other Federal, state, local, or foreign law enforcement, regulatory, or intelligence agencies; personal, identification, criminal history, and other information, including information sources, pertaining to individuals identified as person(s) of interest by Special Agents assigned to the Dignitary Protection Detail; personnel and workload management information. Records include biographical, travel, communication, financial, and surveillance information. To maintain, analyze, and process sensitive investigative information that identifies or may identify criminal noncompliance with Federal tax laws and other Federal laws delegated to CI for investigation or enforcement, and that identifies or may identify the individuals connected to such activity. To establish linkages between identity theft and refund or other tax fraud schemes, and the individuals involved in such schemes, that may be used to further investigate such activity and to perfect filters that identify fraudulent returns upon filing and to facilitate tax account adjustments for taxpayers victimized by these schemes.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

IRS Electronic Tax Administration (ETA) 32

What is the GRS/RCS Item Number?

50

What type of Records is this for?

Electronic

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

Return Review Program (RRP) (SNAP Platform). RRP is used to electronically track, report, monitor, and assign processing of pre-refund tax returns to prevent criminal and civil noncompliance.

What is the disposition schedule?

Cut off RRP data at the end of the calendar year. Retain RRP data in system data tables for 3 years after cutoff, then archive. Maintain RRP archived data until no longer needed.

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?

031

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

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?

Record Control Schedule (RCS)

What is the retention series title?

IRS ELECTRONIC TAX ADMINISTRATION (ETA) 32

What is the GRS/RCS Item Number?

36

What type of Records is this for?

Electronic

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

EFDS provides on-line capabilities to review Electronically Filed Returns (ELF) that have met QRP scoring criteria.

What is the disposition schedule?

Delete when 1 year old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is sooner

Data Locations

What type of site is this?

System

What is the name of the System?

SPLUNK

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

Splunk is a security information and event management (SIEM) and observability platform used to collect, index, search, analyze, and visualize machine-generated data from applications, operating systems, network devices, cloud services, and security tools.

What are the incoming connections to this System?

Application Event Logs

What type of site is this?

System

What is the name of the System?

Enterprise Data Platform (EDP)

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

Enterprise Data Platform (EDP) is a cloud-based platform that centralizes IRS data to support secure data integration, storage, analytics, reporting, and enterprise decision-making.

What are the incoming connections to this System?

COMPASS uses the Palantir Data Connection Agent (PDCA).

What are the outgoing connections from this System?

COMPASS uses the Cloud Security Boundary – External Partner Zone (CSB-EPZ).