Date of Approval: 02/24/2026
Questionnaire Number: 2788

Basic Information/Executive Summary

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

Tax Compliance Check Service, TCCS

Acronym:

TCCS

Business Unit

Privacy, Governmental Liaison and Disclosure

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 Tax Check Program (TCP) includes the Tax Compliance Check Service (TCCS) Application and the Tax Check Application (TCA). TCCS provides Filing and Payment Compliance to many types of customers. Fraud and civil penalty compliance is provided for tax check requests for individuals. Privacy, Governmental Liaison and Disclosure (PGLD) uses the Tax Compliance Report (TCR) created by TCA to respond to valid taxpayer consents submitted by external government agency partners that have a Tax Check Service Memorandum of Understanding (MOU). The Human Capital Office (HCO) utilizes TCA for Personnel Security to verify tax compliance for contractor suitability and background investigations and annually monitors tax compliance of all active IRS contractor personnel. HCO, Employment Talent and Security (ETS) uses TCA to determine employment suitability for all IRS job applicants.

HCO Employee Tax Compliance Office (ETC) obtains data from TCCS to monitor employee tax compliance and determine eligibility for performance award payments. Other IRS offices may utilize TCCS to check tax compliance when a business need arises. The Tax Compliance Report (TCR) is available on demand to taxpayers online via their Individual Online Account (IOLA). The Business Tax Compliance Report is available to business users online via the Business Tax Account (BTA). TCCS has no direct users. It is an application-to-application (A2A) method data exchange. TCCS is a business logic layer that interfaces with the data sources housing tax account information. Tax check requests are sent to TCCS by other applications used by IRS offices. TCCS implements the standard tax compliance criteria established by IRM 25.29.1 IRS Policy Statement - Tax Compliance Check, Standard Tax Compliance Checks for Suitability and Monitoring to ensure fair and consistent treatment of taxpayers. The TCR was designed using plain language to provide taxpayers top quality service by helping them understand their tax check results in an easy-to-read report.

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 Tax Check Program is an IT Program that manages the Tax Compliance Check Service (TCCS) application and includes the Tax Check Application (TCA). TCCS will provide Filing Compliance, Payment Compliance, and Fraud & Civil Penalty compliance data. TCCS is a common enterprise service utilized by multiple applications. TCCS performs tax checks on individual and business taxpayers based on business rules and returns the corresponding tax compliance data in a JavaScript Object Notation (JSON) structure which can be manipulated in different formats by the consumers. TCA processes Comma-Separated Values (CSV) files which lists the requests and creates a TCR in a Portable Document Format (PDF) for successful transactions. The TCCS Consumer application invokes the Tax Check Program Metrics Service to log the results of the TCCS call. The TCRs are transferred to the requesting IRS office via the Enterprise File Transfer Utility (EFTU). The TCCS Consumer application/system invokes TCCS by providing a Taxpayer Identification Number (TIN) (Social Security Number (SSN)/Employer Identification Number (EIN)) and Transaction ID as parameters to receive data. TCCS then calls external systems to get tax data. TCCS has multiple business rules to perform its functionality to determine tax compliance and adjudication data. There will be no data mapping or conversion within TCCS.

The IRS Business Unit owned applications making tax check requests are responsible for any formatting or logic processing compliance data by choosing the interface type. PII data will not be logged in system or event logs. TCCS is limited to providing an automated tax check based on existing tax records. No additional information is collected. TCCS requires the use of SSNs to retrieve the tax records because no other identifier can be used to uniquely identify a taxpayer at this time. TCCS is a non-record keeping system. It is not the official repository for any data or documents. No data is stored.

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

Employer Identification Number
Federal Tax Information (FTI)
Internet Protocol Address (IP Address)
Name
Other
Social Security Number (including masked or last four digits)
Tax ID Number

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

Tax Check Transaction ID

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
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

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)

2

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?

1903

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

Tax Compliance Check Service, TCCS

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.)

Submitting a new PCLIA to include that IP address is collected for the audit trails.

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.

Execution

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.

TCCS reports to the Financial Services Governance Board (FSGB).

9 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

9.1 What is the ABA ID?

211226

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

No

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)

TCCS does not collect information. It only displays existing tax account status to individuals. Due process to address tax liabilities and any federal tax delinquencies is afforded by the Internal Revenue Code and established IRS tax administration procedures. TCCS is not the official repository for any data or documents. Information from the Tax Compliance Report is not used by the IRS for tax administration. The existence of any tax liability reported is based on a previous tax assessment following established IRS procedures with due process rights afforded the taxpayer.

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 system administrators have system access. Access to the TCCS application for IRS administrators is requested via a BEARS (Business Entitlement Access Request System). Access is granted on a need-to-know basis. TCCS does not have any users. It is an application-to-application process. Therefore, no users or managers have system access. There are currently no development activities for TCCS.

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 notifies all individuals who file tax returns via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. IRS functions performing the tax checks are responsible for providing notices to individuals based on the authority used to conduct the tax check. For tax checks provided under the authority of IRC 6103(c), individuals provide a signed Consent to Disclose Tax Compliance Check (Form 14767) which allows disclosure of the information. The individual can decline to sign the consent and stop the process. Form 14767 contains a Privacy Notice stating "We ask for the information on this form to

carry out the Internal Revenue laws of the United States. This form authorizes the IRS to disclose your confidential tax information to the federal agency you appoint. This form is provided for your convenience and its use is voluntary. The information is used by the IRS to determine what confidential tax information your appointee can receive. Internal Revenue Code section 6103(c) and its regulations require you to provide this information if you want to designate an appointee to inspect and/or receive your confidential tax information. Under section 6109, you must disclose your identification number. If you do not provide all the information requested on this form, we may not be able to honor the authorization. Providing false or fraudulent information may subject you to penalties. Routine uses of this information include disclosure to the Department of Justice for civil or criminal litigation and to other federal agencies, as provided by law. We may disclose this information to cities, states, the District of Columbia, and U.S. commonwealths and possessions to administer their laws. We may also disclose this information to other countries under a tax treaty, to federal and state agencies to enforce federal nontax criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. We may disclose this information to persons for purposes of collecting debts through salary and administrative offsets and to the news media as described in IRS Policy Statement 11-94. We may also disclose this information to appropriate persons to assist in responding to compromises of 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?

TCCS does not have any users. Processing is application to application. Only system administrators have system access. Access to the TCCS application for system administrators is requested via a BEARS (Business Entitlement Access Request System). Access is granted on a need-to-know basis. The BEARS enrollment process requires that an authorized manager approve access requests on a case-by-case basis. System administrators are given the minimum set of privileges required to perform their regular and recurring work assignments. They are restricted from changing the boundaries of their access without management approval. System administrator's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the BEARS access.

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

Yes

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.

TCCS adheres to auditing and compliance requirements by leveraging Splunk Security Information and Event Management dashboards for continuous monitoring, security analysis, and vulnerability management, ensuring compliance with IRS cybersecurity standards.

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

Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.

Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Individual Online Account (IOLA)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Financial Management Information System (FMIS)/ Custodial Detail Database (CDDB)

Incoming/Outgoing

Both

Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Enterprise Consolidated Legacy Access System
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

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

Interface Type
IRS Systems, file, or database
Agency Name
Clean Energy (CE)
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type
Other Federal Agencies
Agency Name
Agencies enrolled in the Tax Check Service (attachment uploaded)
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Secure Large File Transfer (SLFT) Business to Business (B2B)

Interface Type
IRS Systems, file, or database
Agency Name
Business Tax Account (BOLA)

Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Application to Application (A2A)

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

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

Interface Type
IRS Systems, file, or database
Agency Name
Business Object Enterprise (BOE)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Application to Application (A2A)

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 24.030 - Customer Account Data Engine Individual Master File
Describe the IRS use and relevance of this SORN.
TCCS performs tax checks. The output is based on a review of an individual's existing tax records.

SORN Number & Name

IRS 26.019 - Taxpayer Delinquent Account Files

Describe the IRS use and relevance of this SORN.

TCCS performs tax checks. The output is based on a review of existing tax records.

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

TCCS performs tax checks. The output is based on a review of existing tax records.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

TCCS produces audit trails to comply with cybersecurity requirements.

SORN Number & Name

IRS 22.061 - Information Return Master File

Describe the IRS use and relevance of this SORN.

TCCS performs tax checks. The output is based on a review of existing tax records.

Records Retention

What is the Record Schedule System?

Non-Record

What is the retention series title?

TCCS It is a non-record keeping system. It is not the official repository for any data or documents.

What type of Records is this for?

Electronic

Data Locations

What type of site is this?

System

What is the name of the System?

Tax Check Program (TCP) Metrics

Please provide a brief description of the System.

TCCS processes tax check requests and then invokes the Tax Check Program Metrics Service to log the results of the TCCS requests.

What type of site is this?

System

What is the name of the System?

SPLUNK

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

Splunk is a Security Information and Event Management (SIEM) software solution tool composed of various dashboards used to aggregate and/or analyze security data for systems/applications used to ensure compliance with IRS cybersecurity standards.

What are the incoming connections to this System?

TCCS sends data to Splunk to adhere to auditing and compliance requirements by leveraging Splunk SIEM dashboards for continuous monitoring, security analysis, and vulnerability management.