Date of Approval: March 29,2018 PIA ID Number: **3304**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Federal Investigative Standards -Tax Check Service, FIS-TCS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Federal Investigative Standards -Tax Check Service, FIS-TCS

Next, enter the **date** of the most recent PIA. 4/17/2017

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
Yes	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
Yes	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Executive Order (E.O.) 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008), and amended January 17, 2017, requires agencies to conduct uniform background investigations for all individuals requiring access to federal facilities; suitability for federal employment, fitness to perform work on a federal contract, and to obtain and maintain a national security clearance. Individuals requiring a Tax Compliance Report for a federal background investigation will access FIS-TCS through a link as directed by the federal investigating agency and authenticate before accessing the FIS-TCS landing page. The taxpayer can view or print the standardized report which indicates whether the individual is tax compliant or non-compliant when tax records reflect a federal tax delinquency. The FIS-TCS Release 1.1 will include an internal application that will allow IRS employees to generate the report upon receiving a signed Consent to Disclose Tax Compliance Check (Form 14767) and release the report as directed by the taxpayer. Release 1.1 will also include enhancements to the report to include a filing information section, tax debts that are outstanding and if any tax fraud penalties were assessed in the last five years.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes	On Primary	No	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. Federal Investigative Standards -Tax Check Service, FIS-TCS requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
Yes	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The FIS-TCS web application allows individual taxpayers to request their own Tax Compliance Report, based on existing tax records, or an IRS employee may generate the report based on a signed Consent to Disclose Tax Compliance Check (Form 14767). FIS-TCS generates a report containing limited information reflecting the individual's current tax compliance status. FIS-TCS

requires the use of SSN's to retrieve the tax records because no other identifier can be used to uniquely identify a taxpayer at this time. The PII from F14767 which includes SSN, name, address and phone number is used to validate the taxpayer against IRS tax records before releasing the tax compliance report.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

Information from the Tax Compliance Report is not used by the IRS for any tax administration purpose; it is made available to the individual for their use. The existence of any tax liability which may be reflected on the report is based on a previous tax assessment following established IRS procedures with due process rights afforded the taxpayer. Tax records for the report are retrieved from the Custodial Detail Database (CDDB) of the IRS which are timely and accurately maintained. CDDB is a subsystem of the Financial Management Information System (FMIS).

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
Treasury/IRS 24.030	Customer Account Data Engine Individual Master File
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/IRS 26.019	Taxpayer Delinquent Account Files
Treasury/IRS 22.061	Information Return Master File

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
eAuth system Information System Continuous Monitoring (ISCM)	Yes	10/07/2015	Yes	02/17/2018
Financial Management Information System (FMIS)	Yes	10/05/2017	Yes	10/27/2017

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Federal Agencies conducting Background Investigations	Taxpayer provides a signed F14767, Consent to Disclose Tax Compliance Check, to allow the tax compliance report to be released	Yes

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
Form 14767	Consent to Disclose Tax Compliance Check

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? No

12b. Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU)

Organization Name	Transmission method	ISA/MOU
Federal Agencies requesting Tax Compliance Reports for Background Investigations	eFax or Batch Processing	Yes

Identify the authority and for what purpose? The FIS-TCS web application allows individual taxpayers to request their own Tax Compliance Report, based on existing tax records, or an IRS employee may generate the report based on a signed Consent to Disclose Tax Compliance Check (Form 14767) - IRC 6103(c).

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? Yes

16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16a1.If **yes**, when was the **e-RA** conducted? 2/28/2017

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

Single Factor Identity Validation

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
The IRS notifies all individuals who file tax returns of such collection 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. Individuals requesting a federal background investigation from an Executive Branch federal agency complete the Office of Personnel Management's Standard Form 85P, Questionnaire for Public Trust Positions or SF 86, Questionnaire for National Security Positions, which provide the required privacy notification and authority to collect PII for

purposes of conducting a background investigation. Consent to Disclose Tax Compliance Checks Form 14767 includes a Privacy Act statement.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s): Individuals may generate the Tax Compliance Report and choose whether to provide it in support their background investigation or provide a signed Consent to Disclose Tax Compliance Check (Form 14767) which allows disclosure of the information. The individual has the opportunity to decline providing the requesting agency a tax compliance report or can decline to sign the consent. The individual can stop the background investigation at any time and stop pursuing employment. It is not mandatory that they continue with the process.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The FIS-TCS application 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.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	No	
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Access is restricted to individuals through a link provided by the federal agency conducting a suitability or security background investigation. The incoming request will be signed by the federal agency conducting the investigation and confirm the identity of the individual as the subject of a background investigation. Access to the FIS-TCS application for IRS employees is requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users 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. The employee'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 OL5081.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

FIS-TCS is a non-record keeping system. No copies of the Tax Compliance Report are being maintained by the IRS. It is not the official repository for any data or documents, and does not require a National Archives and Records Administration (NARA)-approved Records Control Schedule (RCS) to affect data disposition. Audit trail data is maintained in SAAS for seven years in accordance with NARA Job No. N1-58-10-22, approved 4/5/2011 (published under RCS 19 for Martinsburg Computing Center, Item 88).

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 3/9/2018

23.1 Describe in detail the system s audit trail. Audit data is sent to SAAS for certain fields as required by 10.8.3 Audit Logging Security Standards. The logs are then reviewed by Cybersecurity. Only production statistics and Security Audit and Analysis System (SAAS) audit trails necessary for a Moderate impact system will be maintained. FIS-TCS uses the eAuthorization framework for identity-proofing and establishment of identities through credentialing in accordance with National Institute of Standards and Technology (NIST) SP 800-63 requirements.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
Required testing and validation activities are incorporated into Sprint activities following the Agile development scheduling process; all testing for Release 1.0 was completed in September 2017. Testing for Release 1.1 is in process and will be completed in May 2018.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Test results are stored both in DocIT and SharePoint.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?
Yes

If **yes,** provide the date the permission was granted. 6/28/2017

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report