Date of Approval: March 8, 2018 PIA ID Number: **3150**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. eSummons-Secure Data Transport, eSummons SDT

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.

eSummons-Secure Data Transport, SDT, #1103

Next, enter the **date** of the most recent PIA. 2/2/2015

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
No 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
No System Development/Milestone 4B
No System Deployment/Milestone 5
Yes Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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.

eSummons, Secure Data Transport uses two internal IRS process (Secure Data Transport and Enterprise Transfer Utility) to send and receive summons responses from financial institutions (namely banks) electronically. After completing an authentication process, a trading partner such as a bank, is allowed access to the IRS Secure Data Transport (SDT) server where it can download summons request files or upload summons response files to the IRS. Summons response files from banks are temporarily stored on the SDT server before being moved to folders located on a Martinsburg server. Enterprise File Transfer Utility (EFTU) is the internal process that moves files from the SDT server to the group folders. The same process can be used in reverse to send a summons request file to a bank or outside source. A summons file going to a bank is placed by the Revenue Officer (RO) or Revenue Agent (RA) in an outgoing "to" folder, on the Martinsburg server before being picked up and delivered to the SDT server by the EFTU. A unique file naming convention is used to route the files from the Martinsburg server to the SDT server and finally to the trading partner. This unique file naming convention contains specific information about the RO or RA issuing the summons such as their group code and their personal Standard Employee Identifier (SEID). EFTU uses specific characters in the file naming convention to route incoming summons response files to the appropriate folder on the Martinsburg server. To retrieve a summons response file from the bank, the RO, RA or Examiner will access their group folder (one folder for each group) on the Martinsburg server, select their specific summons response file (identified by their SEID) and copy it to their work computer. Group members are granted permissions to access their specific group folder based on their groups organization code. This ensures access to the folders are limited to just employees of a group. Group folder permission to access the folders is controlled systemically based on a link between the folder and HR Connect (a Human Resource system) so that access to the group subfolders are limited to only the employees who are assigned to the group based on a Human Resource (HR) action. This systemic access control is known as Dynamic Folders.

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 Yes On Spouse Yes On Dependent

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

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	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). There is no planned mitigation strategy to mitigate or eliminate the use of SSNs. SSNs may be contained in documents received by the bank which are temporarily stored in this system. Truncation of the Taxpayer Identification Number is not required by the bank when providing a summonsed response file when honoring the summons.

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	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	No
Yes	Place of Birth	No	No	No
Yes	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
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	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	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Summons response files may include various data including: Bank account numbers, Taxpayer addresses- Mailing address. May include other addresses depending on the type of records summonsed. Third Party Data-Depending on the records summonsed, PII information on related third parties may be provided. The summons initiator will advise the summoned bank to provide their summons response electronically. TINs may be provided to help identify the subject of the summons. As summons response files are delivered to a group folder, allowing access to each member of the group, SEIDs will be used in the file naming convention alerting the summons issuer to their file.

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
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
Yes	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.

For the eSummons project, a summons is necessary at times to examine books, papers, records or other data, which may be relevant or material to determine avenues of collection or examination and to ensure taxpayers meet their tax obligations to appropriately report and pay taxes. This data received by the bank, will contain personally identifiable information. The IRS will issue a summons to the bank that may be returned by the financial institution with the files honoring the summons. The summons could include identifying information to assist in identifying the taxpayer as related to compliance cases. Form 6863, the form authorizing the bank to be reimbursed for expenses related to honoring the summons will also contain PII. As summons response files are delivered to a group folder, allowing access to each member of the group, summons initiators SEIDs will be used in the file naming convention alerting the summons issuer to their file.

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

IRS employee are assigned to work the case through to closure. The IRS employee is responsible for resolving any issues/concerns pertaining to the remediation of any discrepancies, which may include issuance of a summons. SEIDs are granted by HR. HR has the responsibility for managing all SEIDs. When the User logs into the system with their SEID and password, if the combination is not correct, the user will not be authorized to access the system. Files are delivered and sent from/to group folders. Through the use of Dynamic Grouping, access to each group folder will be limited only to those employees assigned to the group. Employees outside of the group will not be able to access another group's folder. Exceptions- Requests can be made through the eSummons analyst for access. E.g. an employee detailed to another group would not systemically be given access to the groups folder but may require it. Files received and stored in each group's folder will contain the SEID of the summons initiator alerting them to their file.

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 00.333	Third Party Contact Records
Treasury/IRS 26.019	Taxpayer Delinquent Acct. (TDA) Files
Treasury/IRS 26.020	Taxpayer Delinquency Investigation Files
Treasury/IRS 34.037	IRS Audit Trail and Security System
Treasury/IRS 42.001	Examination Administration File
Treasury/IRS 48.001	Disclosure Records

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? No

11b. Does the system receive SBU/PII from other federal agency or agencies? No

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

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source 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
Financial Institutions	Secure Data Transport	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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? No

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? Yes

If **yes**, identify the other source(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
Third Party Financial Institutions	Secure Data Transport	Yes

Identify the authority and for what purpose? Sources that receive the SBU/PII from system - Third party financial institutions. For each third party financial institution approved to partner with us on this project, an MOU will be secured. Purpose - federal tax administration Authority - Internal Revenue Code (IRC). IRC 7609 provides the Service with summons authority and IRC 7602 provides the Service with special procedures for third-party summonses.

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? No

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?
This change in the way summoned data is received from the bank or how the summons is sent to a bank, does not affect taxpayer's "due process" rights in any way. The taxpayer will continue to receive third party notification of the summons with the ability to quash when appropriate.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? IRC Sec. 7609(i) states the Duty of summoned party. Recordkeeper must assemble records and be prepared to produce records on receipt of a summons to which this section applies for the production of records, the summoned party shall proceed to assemble the records requested, or such portion thereof as the Secretary may prescribe, and shall be prepared to produce the records pursuant to the summons on the day on which the records are to be examined. IRC Sec. 7605 states the time and place of examination pursuant to the provisions of section 6420(e)(2), 6421 (g)(2), 6427(j)(2), or 7602 shall be such time and place as may be fixed by the Secretary and as are reasonable under the circumstances. The summons initiator will advise the summoned bank to provide their summons response electronically. The taxpayer will receive third party notification of the summons with the ability to quash when appropriate.

19. How does the system or business process ensure due process regarding information access, correction and redress?
This change in the way summoned data is received from the bank or how the summons is sent to a bank, does not affect taxpayer's "due process" rights in any way. The taxpayer will continue to receive third party notification of the summons with the ability to quash when appropriate.

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	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read-Only

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The summons response file containing the PII, can be accessed by the initiator of the summons or other authorized employees. Read access only. Through the use of Dynamic Grouping, only employees assigned to each group will have access to the group's folder containing the summons files specifically for group member only. An exception, requested through the eSummons analyst, could be made to allow another to access a groups folder e.g. employee on detail. SEIDs will be used in the file naming convention controlling access to the group folders and alerting the summons issuer that their file is ready for access in the group folder. Access to the outgoing "to" folder for delivery of the summons file to the bank will not be restricted to just those in a particular group. IRS users will have read/write access to the "to" folder. However, files will only be stored in the "to" folder for no longer than 10 minutes before the file is picked up by EFTU and moved to the SDT folder. 10 minutes is the standard used by the Files Transfer Unit. The eSummons program analyst will have read/write access to all folders including all group folders as well as administrative folders to include the outgoing folder, incoming folder, archive folder and reject folder.

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? No

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.

Information Technology's eSummons Project/General Support System (GSS-17) is non-recordkeeping. GSS-17 provides a platform for secure eSummons communications and information sharing, but it is not the official repository for any data or documents. Files will be stored only temporarily. After accessing the summoned file from the Martinsburg Server, the IRS employee (generally the employee who issued the summons) will copy the file to their work computer. The employee will then delete the file stored on the server. It is not expected to remain on the server for more than 60 days. Upon closing of the case, the summoned file will be removed/deleted from the IRS SB/SE employee’s computer. All case-related information will be stored in a central repository and will be retained: (a) for up to 10 years after the case is closed as required by IRS Document 12990 under Records Control Schedule (RCS) 28 for Tax Administration-Collection, item 6 for Case Files; or (b) for up to 10 years after the case is closed as required by IRS Document 12990 under RCS 23 for Tax Administration-Examination, item 42 for Examination Case Files.

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)? Yes

23a. If **yes**, what date was it completed?

23.1 Describe in detail the system s audit trail. Continuous Monitoring procedures are in place for the GSS. These procedures are completed annually to ensure the application and its data are properly secured. In addition, the Security Assessment and Authorization (SA&A) process is completed every three years or when a significant change is made to the system.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. This is not a new system so does not require testing. Files are regularly exchanged using this process.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	50,000 to 100,000
26b. Contractors:	Not Applicable
26c. Members of the Public:	Under 100,000
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? Yes

If **yes**, 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? Contact ***Disclosure*** to determine if an accounting is required. No

30a**.** If **no**, accounting of Disclosures risk noted. Contact ***Disclosure*** to develop an accounting of disclosures. Explain steps taken to develop accounting of disclosures process. No accounting required for investigative disclosures per IRC 6103(p)(3)(A).

End of Report