A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: July 21, 2015 PIA ID Number: **801**

1. What type of system is this? New

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Taxpayer Digital Communications, TDC

2a. Has the name of the system changed? No

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Under 5,000
Members of the Public:	Under 100,000

4. Responsible Parties: N/A

5. General Business Purpose of System

As communication between the IRS and the taxpayer continues to grow, the IRS has a need for new technologies to more efficiently communicate via new Internet-based technologies. These technologies will allow the IRS to significantly lower costs by reducing paper mail correspondence and deflecting phone calls and walk-in visits as well as enhance the taxpayer experience by offering more modern ways of communicating. IRS has initiated a program called Taxpayer Digital Communications (TDC). This Project is in response to IRS employees, taxpayers, and third party organizations requesting more modern, efficient, and secure ways to communicate and transfer digital documents. Modernization with digital communication channels will allow IRS employees to resolve taxpayer issues more efficiently. The IRS TDC program will set goals to decrease the amount of time taxpayer cases are open, significantly lower communication costs, reduce operational risks, and increase taxpayer satisfaction scores. The principal goal of this project is to provide best-in-class service, deliver high quality examinations, and a consistent communication experience across all IRS lines of business.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) No

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. none

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	Yes	
		Other Source:
Other	No	

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Social Security Number (SSN)	Yes	No
Name	Yes	Yes
Taxpayer Identification Number (TIN)	Yes	No
Address	Yes	No
Date of Birth (DOB)	Yes	No
Telephone Number	Yes	No

10a. What is the business purpose for collecting and using the SSN ?

This information will be used for various compliance exams, application submission, case correspondence, and other communication and artifacts that need to be sent to and from Taxpayer and IRS employees. SSN, TIN, PTIN, will also be used to correlate relationships between a Taxpayer and their POA representative. SSN, personal email, first name, last name, and cell number will be provided to the TDC system via the existing eAuthentication system.

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

26 U.S Code 6109 – Identifying Numbers The Paper Reduction Act of 1980 and 1995. See 'purposes': http://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm Treas. Reg § 301.6103©-1(b) – disclose returns or return information to designated third parties where the consent is not for the purpose of assisting the taxpayer to resolve a tax matter. Treas. Reg. § 301.6103(c)-1(c) contains the requirements for requests made by the taxpayer to other persons, such as a Member of Congress or a relative, for information or assistance relating to the taxpayer's return or a transaction or other contact between the taxpayer and the IRS. Consents under this provision may be in writing or oral. Tax Reform Act of 1976 (Pub. L. No. 94-455, section 1211), expressly exempts state agencies from this restriction to the extent that SSNs are used "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction."

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

Masking is an option for the body of an email that may be used to avoid having SSN, TIN, or PTIN on the primary messages seen in the TDC platform. The goal is to mirror the paper process so where SSN is shown on paper forms the plan is to show the same in the body of the secure message. These could be masked by only showing the last 3 digits of a SSN, TIN, or PTIN where the data is not fully shown. It may be possible to avoid using SSN alltogether, however there would be nothing to limit any taxpayer or practitioner to send this type of information via the Secure Message platform.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

Eliminating the SSN on the system may be challenging due to the nature of the information that needs to be sent back and forth between the IRS and TP or Tax Prepares. Masking the body of the secure message is achievable, however the nature and content of information in attachments and artifacts could contain SSN data.

Describe the PII available in the system referred to in question 10 above.

This solution will transmit similar information that is currently sent via USPS for audits, exams, and any case open between the IRS and Taxpayer. This could include any and all types of PII.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

The system will record and store every message sent between a taxpayer and IRS employee. Any click or activity that is done by a taxpayer or an IRS employee will also be recorded and available in pre-defined reports as well as the ability to export into a separate audit system.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
RGS	Yes	04/23/2012	No	
AIMS	Yes	04/03/2012	No	
TAMIS	Yes	07/02/2014	No	
eAuthorization	Yes	01/29/2013	No	
IDRS	Yes	08/03/2014	No	
xPression	No	08/03/2014	No	
CEAS	Yes	09/17/2012	No	

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: Yes

If yes, the third party sources that were used are:

Power of Attorney information, electronic bank statements, electronic copies of lease agreements, digital images of birth certificate from hospitals are examples of third party sources.

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: No

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

There are multiple business needs for the collection of PII in the system based on IRS Business Operating Division (BOD) use case and needs. Since this is a communication platform, there are multiple document types that will contain PII similar to what is currently contained in correspondence via the United States Postal Service (USPS). For example, for the Wage and Investment (W&I) BOD, the TDC platform will be use for Compliance

Correspondence Exams. The type of information that will be requested of the taxpayer is simlar to what happens today via an exam that is done via USPS. The taxpayer may need to send in digital copies of bank statements, mortgage information, birth certificates, medical records, and charital contribution documents. Similar digital documents could be requested from Small Business/Self-Employed (SBSE) for equivalent small business data which may include TIN, bank statements, receipts etc. Other BOD's may have additional PII level information requests including Tax Exempt & Government Entities (TEGE), Large Business & International (LB&I), and principal offices including Taxpayer Advocate Service (TAS) and Return Preparer Office (RPO). These all may have unique PII equivalents that will utilize the secure digital transfer of documents features in the TDC platform. TAS for example could request PII levels of information for a Taxpayer to prove a proof of hardship. This may include bank and financial information as well as lease agreements and dependent information.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes	
To provide taxpayer services	Yes	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? Yes

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	Yes	OMB Memorandum 10-22
Web Beacons	No	
Session Cookies	Yes	
		If other, specify:
Other:	No	

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If **Yes**, how is their permission granted?

The taxpayer will be invited by the IRS to use the system and register via IRS eAuthentication system. Once they have validated their identity in eAuth, they will be asked to opt-in to access the TDC platform with the necessary terms and conditions for the requested use of the information.

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

The TDC system will be accessed by IRS employees that will receive and analyze any PII information that is contained in electronically transferred documents. Processes will be put in place to ensure 'due process' is followed

as it is done today via paper correspondence. If a taxpayer views any information as being incorrect, they will be able to communicate with IRS personnel to make the requisite changes. As TDC is only a message exchange platform, the official information will remain in today's existing systems.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

ID	Form Number	Form Name
3481	911	Request for Taxpayer Advocate Service Assistance
3482	CP566	Examination Issue notice
3484	CP521	Installment Agreement Payment Due
3485	4549	Income Tax Discrepancy Adjustment
3486	3219	Notice of Deficiency
3487	525	Taxable and Non Taxable Income
4986	cp2000	Automated Under Reporter

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: Contractor Owned and Operated

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		Read Write
System Administrators		Read Only
Developers		Read Only
Contractors:	Yes	
Contractor Users		Read Write
Contractor System Administrators		Read Only
Contractor Developers		Read Only
Other: Taxpayers & Practitioners will be able to post messages and upload digital artifacts into the system	Yes	Read Write

If you answered yes to contractors, please answer **22a.** *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

Taxpayers will need to go through the IRS eAuthentication solution and 'opt-in' to digital communications. The eAuthentication solution will provide the authorization parameters for who has access to what components of the TDC platform. IRS employees will have access to the system to use as a tool to interact with Taxpayers. Their management and supervisor will provide the authorization for employees to have access to the TDC platform. They will they set up login credentials to interact with the system.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

At this time, the PII will be contained in secure online messages and in certain digital artifacts. These will come in multiple forms and will not be aligned with any specific database element. There will be case identifiers and possibly SSN/TIN that will be stored as part of the case information that is stored in the TDC platform. This will be verified and cross checked with the source system/data owner for accuracy and completeness. The intent if for TDC is to utilize existing source systems and relationships and not to be the system of record for any manipulated or changed PII. TDC will primarily serve as a communication channel between the Taxpayer and the IRS replacing the paper channels used today.

25. 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

25a. 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.

TDC Pilot records (TDC information and artifacts received from taxpayers) are unscheduled and will be stored indefinitely until determined otherwise. The IRS Records Office and system owner will draft and submit to the National Archives a request for records disposition authority. The Records Office proposes a short-term retention for pilot correspondence data that not only covers this pilot, but would apply to the adoption/documentation of potentially new future procedures, TDC project files. The processing of pilot examinations is not affected in any way. Guiding retention considerations will be current correspondence exam IRM 4.71.16.12 (06/07/2012) Record Retention Requirements 4.71.16.12.1, and Records Control Schedule (RCS) 23 guidance for Tax Administration Examination records published in Document 12990. RCS 23, Item #42 B states that Coordinated Examination Case files must be retired to the Federal Records Center (FRC) 4 years after the date of closing and should be destroyed 15 years from the date of closing. Closing is defined as when the case is posted on AIMS to status 90 but also includes procedures for processing the agreed portion of workpapers when Appeals or Area Counsel does not want them. It is important that appropriate procedures be established to permit the retrieval of prior EPTA Examination Files (Historical Files) from the FRC. For example, it may be necessary to obtain previously closed files in the event that an EPTA Examination case is post reviewed by Treasury Inspector General for Tax Administration (TIGTA) or the Governmental Accounting Office. In addition, taxpayers may file claims with respect to various federal tax issues previously closed at the Examination or Appeals levels and retrieval of the documents may be necessary. These records disposition rules as they apply to TDC will be reviewed with the IRS Records Office, as well as appropriate recordkeeping format for any TDC “born electronic” correspondence.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
The PII will be included in digital documents and stored via a FedRamp certified data center via software that is FISMA certified. All access to taxpayer PII will approved by management and vendor agreements. All communication will be transferred at a minimum via SSL or higher encryption. For vendors providing SaaS or managed services at facilities outside of an agency’s direct control, it is a federal requirement that they are FedRAMP (Federal Risk and Authorization Management Program) certified. Operated by the GSA, the FedRAMP program ensures that technology and services vendors meet relevant NIST security guidelines and follow government procedures for security auditing, site regulation, personnel management, etc. FISMA refers to the Federal Information Security Management Act of 2002 which sets requirements for the treatment of information within federal IT systems. NIST(National Institute of Science & Technology) sets the standards and levels of compliance for various technologies and system implementations. For TDC, the required level of FISMA certification of the TDC vendor platform will be “FISMA-Moderate”..

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Data in the system will be encrypted while at rest in the system. Any data that data in transit will be done via cyber agreed secure network processes.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

When the final system is procured, a full SA&A will be conducted. It will also have ongoing security checks and at least one SA&A done per year for the length of the contract.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORN Number	SORN Name
Treas/IRS 00.001	Correspondence
Treas/IRS 34.037	Audit Trail and Security Records System

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	Yes
New privacy measures have been considered/implemented	Yes
Other:	No

32a. If **Yes** to any of the above, please describe:

We will investigate masking any SSN or PII information when possible or determine if storing PII is absolutely necessary in conducting the correspondence between the taxpayer and the IRS. Online retention rules will also be discussed to determine any new privacy policy to account for online data retention.