Date of Approval: **September 01, 2020**

PIA ID Number: **5188**

## SYSTEM DESCRIPTION

*Enter the full name and acronym for the system, project, application and/or database.*

Taxpayer Digital Communications, TDC

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym and milestone of the most recent PCLIA?*

Taxpayer Digital Communication, TDC, 3470, Approved

*What is the approval date of the most recent PCLIA?*

11/9/2018

*Changes that occurred to require this update:*

Significant System Management Changes

Significant Merging with Another System

New Access by IRS employees or Members of the Public

*Were there other system changes not listed above?*

No

*What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.*

WebApps Governance Board

*Current ELC (Enterprise Life Cycle) Milestones:*

Detailed Design/Milestone 4A

System Development/Milestone 4B

Operations & Maintenance (i.e. system is currently operational)

*Is this a Federal Information Security Management Act (FISMA) reportable system?*

Yes

## GENERAL BUSINESS PURPOSE

*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.*

The IRS is leveraging new technologies to more efficiently and securely communicate digitally with taxpayers and tax professionals. This technology includes the following secure digital communication capabilities: 1. Secure Messaging: Taxpayers and IRS representatives can send and receive messages via a secure web-based online portal with the option for notifications and attachments. Good for supplementing mail correspondence. 2. Text Chat: Taxpayers can initiate online chats with an IRS representative from within a secure portal. Useful alternative to phone interactions. 3. Virtual Assistant: Conversational virtual agent providing a unique, interactive, and personal way for users to get answers and assistance 24 hours a day, 7 days a week. Useful for deflecting phone contacts and pre-screening text chats. These technologies will allow the IRS to lower costs by reducing paper mail correspondence, deflect phone calls and walk-in visits, and enhance the taxpayer experience by offering more digital options for communications. This will also provide the capability to transmit documents between the IRS and authorized external parties. Information securely transferred via these channels will be used to help resolve taxpayer issues, expedite IRS exam cases, and enable sending and receiving digital documentation between the IRS and external parties. Areas of IRS that will benefit from these new communication channels are Small Business Self-Employees (SBSE), Large Business & International (LB&I), Wage and Investment (W&I), Independent Office of Appeals, Tax-Exempt Governmental Entity, Chief Counsel, Criminal Investigation and others.

## PII DETAILS

*Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?*

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

*What types of tax identification numbers (TIN) apply to this system?*

Social Security Number (SSN)

*List the approved Treasury uses of the SSN:*

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

*Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)*

SSN is passed by IRS Secure Access during the authentication and authorization process for individual taxpayers and Powers of Attorney. The SSN in the system is also used for IRS exams to align documents required with the taxpayer. It is also used to provided support services to taxpayers to authenticate them for access to account level information.

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

The TDC platform does provide the ability to mask PII information such as SSN's and Preparer Tax Identification Number (PTIN)S for live chat session. However, due to the content that is transmitted back and forth there is no plan or ability to eliminate the transmission of documents that contain PII such as SSN's and PTINS.

Employer Identification Number

Other Taxpayer Identification Number

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

Yes

*Specify the PII Elements:*

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Financial Account Numbers

Employment Information

Tax Account Information

Centralized Authorization File (CAF)

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

Yes

*Specify the types of SBU from the SBU Types List*

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.

Proprietary data Business information that does not belong to the IRS

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

*Are there other types of SBU/PII used in the system?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Any information that is currently sent via US or international mail, fax, or provided in a face to face environment for any IRS audit or IRS support case will be able to be securely transmitted digitally via TDC if that information is in a digital format. System level information includes user id's, case id's, activity id's, log files, command codes, activity dates, activity types which could be considered SBU.

*Cite the authority for collecting SBU/PII (including SSN if relevant*

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

*Has the authority been verified with the system owner?*

Yes

## BUSINESS NEEDS AND ACCURACY

*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.*

Specific use of SBU/PII will be based on the IRS Business Operating Division (BOD) or Functional Operating Division (FOD) use case needs (like correspondence examinations, audits, etc.), system and process training, and standard operating procedures of the user groups. As this is a communication platform with file sharing capabilities, there are multiple document types that will be exchanged. These document types will contain the same or similar SBU/PII as what is currently contained in traditionally paper-based file sharing methods like correspondence via US or International mail, faxes, or documents provided via face-to-face meetings. Instead of these traditional methods, such documents will be sent and received either via Secure Message or Secure Chat but only after the taxpayer or authorized representative has fully authenticated via IRS Secure Access or other approved methods such as a signed Consent Agreement.

*How is the SBU/PII verified for accuracy, timeliness and completion?*

The TDC system will be accessed by IRS employees that will receive and analyze any PII information that is contained in electronically transferred documents. Current and new processes will be used to verify for accuracy, timeliness and completeness. Guidelines for this will be similar to paper processes since documentation sent digitally is the same materials that previously were sent via paper mail or fax.

## PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

*Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.*

Yes

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 34.037 Audit Trail and Security Records

## RESPONSIBLE PARTIES

*Identify the individuals for the following system roles:*

## Official Use Only

## INCOMING PII INTERFACES

*Does the system receive SBU/PII from other systems or agencies?*

Yes

*Does the system receive SBU/PII from IRS files and databases?*

Yes

*Enter the files and databases:*

System Name: IRS Secure Access/eAuthentication
Current PCLIA: Yes
Approval Date: 11/9/2018
SA&A: Yes
ATO/IATO Date: 2/21/2020

System Name: IRS Active Directory Federation Service (ADFS)
Current PCLIA: No
SA&A: No

*Does the system receive SBU/PII from other federal agency or agencies?*

No

*Does the system receive SBU/PII from State or local agency (-ies)?*

No

*Does the system receive SBU/PII from other sources?*

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: Various IRS Case Management Systems such as Report Generation System (RGS), Correspondence Exam Automation Support (CEAS), Integrated Data Retrieval System (IDRS), Automated Underreporter (AUR) case management, & Appeals Centralized Database System (ACDS)
Transmission Method: Manually typing into chats or secure messages or attaching documents to messages
ISA/MOU Yes

*Does the system receive SBU/PII from Taxpayer forms?*

No

*Does the system receive SBU/PII from Employee forms (e.g. the I-9)?*

No

## DISSEMINATION OF PII

*Does this system disseminate SBU/PII?*

Yes

*Does this system disseminate SBU/PII to other IRS Systems?*

Yes

*Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.*

System Name: Splunk
Current PCLIA: Yes
Approval Date: 1/27/2020
SA&A: Yes
ATO/IATO Date: 3/28/2017

*Identify the authority*

The interface with Splunk is by request of the IRS Chief Information Officer (CIO).

*For what purpose?*

Per direction from the IRS CIO, this interface will generate TDC platform log files to identify potential unauthorized access (UNAX) violations. The details logged for each event may vary widely, but at minimum each event should capture timestamp; event, status, and/or error codes; service/command/application name; user or system account associated with an event. The solution shall transfer audit log data files once per day from the private cloud to a secure file transfer protocol (FTP) site where files can be picked up by IRS and ingested into the IRS Splunk application for analysis.

*Does this system disseminate SBU/PII to other Federal agencies?*

No

*Does this system disseminate SBU/PII to State and local agencies?*

Yes

*Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).*

Organization Name: All State and Local Agencies that communicate with Tax Exempt and Government Entities (TEGE) Business Unit
Transmission Method: Secure Message
ISA/MOU Yes

*Identify the authority*

IRC 6103 (d) provides that tax information may be shared with state and local agencies responsible for tax administration. The IRS WebApps Governance Board also approved implementing secure messaging for this use in May 2018.

*Identify the Routine Use in the applicable SORN (or Privacy Act exception)*

IRS 00.001 - Correspondence Files and Correspondence Control Files

*For what purpose?*

Examining bond issuer for examination of tax issues arising from tax bonds.

*Does this system disseminate SBU/PII to IRS or Treasury contractors?*

No

*Does this system disseminate SBU/PII to other Sources?*

No

## PRIVACY SENSITIVE TECHNOLOGY

*Does this system use social media channels?*

No

*Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?*

No

*Does the system use cloud computing?*

Yes

*Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?*

Yes

*Date Certified*

6/21/2016

*Please identify the ownership of the CSP data.*

Third Party

*Does the CSP allow auditing?*

Yes

*Who audits the CSP Data?*

IRS

*What is the background check level required for CSP?*

Moderate

*Is there a breach/incident plan on file?*

Yes

*Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:*

Storage

Transmission

Maintenance

*Does this system/application interact with the public?*

Yes

*Was an electronic risk assessment (e-RA) conducted on the system/application?*

Yes

*When was the e-RA completed?*

11/30/2016

*What was the approved level of authentication?*

Level 3: High confidence in the asserted identity's validity

## INDIVIDUAL NOTICE AND CONSENT

*Was/is notice provided to the individual prior to collection of information?*

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?*

Upon first entry to the TDC platform, individuals must agree to a 'Terms of Service' (TOS) before continuing to use secure messaging. The TOS has been fully approved by IRS Counsel Office, IRS Privacy, Governmental Liaison and Disclosure group, and IRS Online Services. Any change to the TOS will require any current or new taxpayer that accesses the

system to agree to updated language before continuing to use the TDC system. For Chat, a message is displayed in the pre-chat screen with legally approved language before starting a chat session.

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

Yes

*Describe the mechanism by which individuals indicate their consent choice(s):*

An individual does have the ability to decline using the system after reading the TDC Terms of Service (TOS). Also, at any time, the taxpayer can refuse to provide any information via TDC and continue to use fax, mail, or in person communications. TDC provides alternative communication channels and does not limit use of existing channels such as mail, fax, or phone.

*How does the system or business process ensure 'due process' regarding information access, correction and redress?*

The TDC system will be accessed by IRS employees that will receive and analyze any information that is contained in the electronically transferred documents. Processes are currently in place to ensure 'due process' is followed as it is done today via phone, mail, or in-person communications. These processes may be modified for TDC but the rules for handling PII are the same. If a taxpayer views information as being incorrect, they will be able to communicate with IRS resources to make the requisite changes. TDC is a communication platform only, the official case or tax information will remain in current IRS systems of record. IRS users also need to submit an Online 5081 (OL5081 an IRS System) that is approved by management before being granted access to the system. Once access is granted, each user of TDC is granted permission and roles that only allow them to see what they have permission for. Finally, all access to customer data is auditable with full tracking capability.

## INFORMATION PROTECTION

*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 Contractor Operated

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

*IRS Employees*

Users: Read Write

Managers: Read Write

*IRS Contractor Employees*

Contractor System Administrators: Administrator

Contractor Developers: Read Only

*How is access to SBU/PII determined and by whom?*

Access to the system is provided via OL5081 request which is then sent to IRS Online Services (OLS) for approval. Required and OLS management approved resources will have access to the system and a full audit trail is provided for any new account activations or deactivations.

## RECORDS RETENTION SCHEDULE

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?*

Yes

*How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.*

TDC records owners and developers are working with the IRS Records Office to draft data retention requirements for submission to/approval by the National Archives and Records Administration (NARA). All records managed in TDC must be preserved until retention periods are finalized and approved by NARA. RCS 11 Item 1-14 RCS 29 Item 447

## SA&A OR ASCA

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

Yes

*What date was it completed?*

8/20/2019

*Describe the system's audit trail.*

The system has a very detailed audit trail that is accessible and reportable. This is based on 2 primary system actions. The first is an 'activity'. An activity is a unit of work that may be a task, created to track an internal work item. It could also be an interaction between a taxpayer and an IRS agent or an interaction between a supervisor and an IRS agent. These are all tracked in detail with a time and date stamp. All activities have a unique 'activity ID' assigned to them. The second is a 'case'. A case is used to group activities related to the same issue. Activities are tied to a case using a single identification number, the 'Case ID'. A case contains activities of various channels such as secure messages, email notifications, chats, phone, or internal tasks. There is an 'audit' function of an activity that shows every single action that has occurred on an activity. It gives complete information from the moment the activity was created to where the activity is at present. Supervisory activities are also included in the audit information.

## PRIVACY TESTING

*Does the system require a System Test Plan?*

Yes

*Is the test plan completed?*

No

*When is the test plan scheduled for completion?*

9/15/2020

*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?*

The platform is a Commercial Off-the-Shelf System (COTS) and is licensed in an already approved and system tested state. Additional system tests are frequently performed for maintenance and functional releases. For the new interfaces for file share and IRS Personal Identification Verification (PIV) card integration, these system tests will be performed in conjunction with IRS and Information Technology (IT) and are planned to be completed by 09/15/2020.

## SBU DATA USE

*Does this system use, or plan to use SBU Data in Testing?*

No

## NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: 100,000 to 1,000,000

Other: No

## CIVIL LIBERTIES

*Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?*

No

*Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*

No

*Will this system have the capability to identify, locate, and monitor individuals or groups of people?*

No

*Does computer matching occur?*

No

## ACCOUNTING OF DISCLOSURES

*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

*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.*

Yes