Date of Approval: **September 25, 2019**

PIA ID Number: **4408**

SYSTEM DESCRIPTION

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

Taxpayer Digital Communication - Outbound Notifications, TDC-ON

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?

TDC-ON, PIA #2618

What is the approval date of the most recent PCLIA?

5/19/2017

Changes that occurred to require this update:

Expiring PCLIA

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.

Web Applications Governance Board Strategic Development Executive Steering Committee (SD-ESC)

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

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.

TDC-ON Release 1 (R1) is a Web-based application that will allow individual taxpayers access to specific IRS notifications using a single sign-on capability. TDC-ON will leverage the existing IRS eAuthentication, Web Apps Online Account (OLA), and Web Apps Platform capabilities to authorize access and manage online functionality. The scope of TDC-ON (R1) consists of designing the TDC-ON architecture, deployment of the infrastructure, creation of a TDC-ON account structure or wrapper to view the specific features and the development and deployment of the following functionality:
* View a Message Center with a list of prior Notice Conversion (NOTCON) notices (as of deployment date)
* View/Download select notices which NOTCON has converted to an accessible format and made available to TDC-ON
* Provide taxpayers access to a set of official notices in PDF format that they can view and download from their OLA account. TDC-ON is not in Operations & Maintenance, we are in development milestone 2 (MS2). As an Agile ELC path we are working towards Product Planning Review exit for new development.

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:

Another compelling reason for collecting the SSN

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

The only use of SSN is the view of the SSN that may be present on some of the digital notices sent to the taxpayer, although most notices mask the SSN.

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

There are no current plans for TDC-ON to eliminate the use of SSN's. However, all taxpayer interactions that involve sharing of SSN information will be via HTTPS protocols and will require the taxpayer to create an online user id and password via the eAuthentication system to access TDC-ON.

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

Date of Birth

Tax Account Information

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 (SBU List)

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.

Federal Tax Information

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.

They system uses SBU/PII and SSN's for the administration of taxpayer account data and tax account payment information.

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

SBU/PII is verified for accuracy, timeliness and completeness via the use of the eAuthentication system to validate taxpayer identity prior to access to online systems. The TDC-ON system will not store SBU/PII outside of current IRS data stores and systems such as the Integrated Data Retrieval System (IDRS).

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 System

IRS 24.030 Customer Account Data Engine Individual Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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: Notice Conversion

Current PCLIA: Yes

Approval Date: 11/1/2016

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?

No

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?

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?

No

Does this system/application interact with the public?

Yes

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

No

When will the e-RA be completed?

10/30/2019

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?

The irs.gov has several methods of informing the taxpayer about these issues. The irs.gov website has a Privacy Policy which states "Using these services is voluntary and may require that you provide additional personal information to us. Providing the requested information implies your consent for us to use this data in order to respond to your specific request." Prior to using the Where's My Refund (WMR) application, WMR has the required notice that this is a US Government system for authorized use only.

The application requires that the taxpayer acknowledge that Internal Revenue Code Section 6109 authorizes the collection of the social security number in order to provide the service requested by the taxpayer. The application also informs the taxpayer of use of the System of Records 24.030 Individual Master File. The taxpayer is also provided a link to all IRS Privacy Impact Assessments.

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):

The taxpayer's use of the web application is voluntary. The taxpayer/user must click on the "Consent" button to the notice provided on the website before being allowed to proceed. Authentication is required in order to have confidence in the identity of the web application user.

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

The taxpayer has due process by calling, faxing, or visiting the IRS with regards to information access, correction, and redress.

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 Operated

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

IRS Employees

System Administrators: Read Write

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

Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets for the purpose of authentication. Once they enter shared secrets and their data matches up with the Integrated Data Retrieval System information to ensure that the information is correct, they are eligible to use the system. IRS System Administrators are provided access to the servers thru the Online 5081 (OL5081) system. Access to the data is determined by the manager based on a user's position and need-to-know. This requires the supervisor to authorize the access to the server or servers.

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.

All records housed in the Taxpayer Digital Communication-Outbound Notifications System will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data. Any new records generated by the system will be managed according to requirements under Internal Revenue Manual (IRM) 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedules (RCS) 29, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. Balance Due Notices (IRS correspondence) are scheduled under RCS 29, Item 69(2) Payment of Taxes Records are scheduled under RCS 29, Item 136.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

TDC-ON will work with the Enterprise Security Audit Trails (ESAT) team to define and audit requirements, leverage and supplement those requirements with ESAT Audit Plan where applicable and send the appropriate logs to the Security Audit and Analysis System (SAAS). Expected to be completed during Milestone 4, before May 2020. TDC-ON is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Web Applications Testing System Integration Plan (serving as the System Test Plan (STP) for TDC-ON) is stored in the Web Applications SharePoint.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

Only the PII that is needed to authenticate is requested from the taxpayer. The validation process will verify the accuracy and completeness of the information in accordance with the business rules. Authentication is tested thoroughly to ensure security and confidentiality. An audit trail ensures that all users activities are being monitored. The results of the test cases are documented and analyzed for defects.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 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?

No