

Date of Approval: **June 08, 2020**

PIA ID Number: **5092**

SYSTEM DESCRIPTION

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

IRS2Go, IRS2Go

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?

IRS2Go

What is the approval date of the most recent PCLIA?

6/28/2017

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

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.

Strategic Development Executive Steering Committee (SD ESC)

Current ELC (Enterprise Life Cycle) Milestones:

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

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

No

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.

IRS2Go is the IRS mobile application for smartphones and tablets running iOS or Android. IRS2Go allows users to check on the status of their tax refund, have easy access to mobile-friendly IRS payment websites, sign up for tax tips, check nearest volunteer income tax assistance locations, contact us, or set up a "second factor" authenticator for their eAuthentication (Secure Access) account. IRS2Go is a mobile app frontend used to access existing IRS systems already available on the internet & inherits/obeys whatever requirements these applications already enforce; IRS2Go is not a system itself.

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:

When there is no reasonable alternative means for meeting business requirements

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

SSN is required for certain applications such as Where's My Refund. IRS could not provide the service without it.

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

N/A - IRS2Go is just a mobile frontend for other IRS services that may require use of SSNs.

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:

E-mail Address

Tax Account Information

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

No

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.

Users of IRS2Go may provide their email address to subscribe to IRS newsletters, which are managed through GovDelivery. Email addresses provided through IRS2Go to GovDelivery are not stored by IRS2Go or any IRS system, and are passed directly to GovDelivery. This is completely voluntary and is only provided by users interested in subscribing to IRS email newsletters. Users of eAuthentication may set up multi-factor authentication security code capabilities through the IRS2Go app. To do this, users may enter their eAuthentication username into IRS2Go. The username is transmitted between IRS2Go and eAuthentication and is stored on the user's mobile device using IRS2Go. This is completely voluntary and is only provided by users interested in obtaining security codes from IRS2Go instead of using SMS text messages.

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.

The public user or taxpayer provides the information on a voluntary basis if they are seeking certain information from the IRS. They must provide PII about themselves to receive these services. The information they provide is matched against taxpayer information from IRS tax systems to authenticate the user and to provide the information requested. For services that do not require identification (ID) of the user, no PII is requested, used or stored. The taxpayer provides requested PII. The information entered by the user is matched against retrieved information to authenticate the user. IRS2Go does not store SSNs on-device; SSNs are provided directly to the web service requested by the user (such as Where's My Refund).

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

The PII in the system is used only for authentication purposes and mirrors the Where's My Refund web application using similar controls. A Secure Access username is voluntarily collected if a taxpayer uses any features in IRS2Go tied to the eAuthentication (Secure Access) service, which uses usernames to identify a taxpayer's account.

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 24.030 Customer Account Data Engine Individual Master File
- IRS 34.037 Audit Trail and Security Records
- IRS 00.001 Correspondence Files and Correspondence Control Files
- IRS 24.046 Customer Account Data Engine Business Master File

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: Where's My Refund
Current PCLIA: Yes
Approval Date: 2/13/2018
SA&A: Yes
ATO/IATO Date: 3/27/2017

System Name: eAuthentication
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 10/24/2017

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.?

Yes

Briefly explain how the system uses the referenced technology.

Geolocation may be used within iRS2Go. The application resides on an end user's mobile device and connects to IRS systems to retrieve and display information in a similar manner to Volunteer Income Tax Assistance (VITA) locator web application. Users of the VITA locator may select to search for nearby VITA locations based on their device's GPS feature. This is completely voluntary, and if selected, IRS2Go asks for the user's acknowledgement before retrieving location data. The location data is only used to retrieve the user's ZIP code for the VITA locator, and location data is not stored or used for any other manner.

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?

Not Applicable

Please explain.

IRS2Go is not a system itself; IRS2Go is just a frontend to access other systems. Electronic Risk Assessments or Digital Identity Risk Assessments (DIRA) are performed on the underlying systems that provide data to users through IRS2Go (for example, the DIRA assessment for Where's My Refund covers the use of Where's My Refund through the IRS2Go mobile app frontend).

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?

A privacy notice is provided within the IRS2Go app, using same language as on the Where's My Refund website.

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):

Use of the IRS2Go application is completely voluntary. Individuals can choose not to use the system to check their refund status, and no information will be collected.

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

The Taxpayer Bill of Rights outlines the baseline for 'due process'. IRS2Go is not a data source or system itself; any corrections would be handled with the processes of the system that IRS2Go interacts with (e.g. Where's My Refund).

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:

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

Not Applicable - IRS2Go does not store SBU/PII. Any SBU/PII is passed directly to another system, such as Where's My Refund or eAuthentication, securely over the internet. Access to SBU/PII is handled by that system's policies.

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.

IRS2Go is non-recordkeeping. It is a mobile application used to collect and display information from other, existing IRS.gov services on mobile devices. It is not a data repository system. Any records, such as those associated with retrieving a taxpayer's refund status, are kept in that system's own logs (for example, Where's My Refund/Internet Refund Fact of Filing) - the same as if the taxpayer had visited the IRS.gov website to perform the same task.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

6/30/2020

Describe the system's audit trail.

As part of the ELC, IRS2Go is required to receive approval through the SA&A process prior to release. IRS2Go cannot be released without receiving SA&A approval during the ELC milestone exit process. There is no audit trail for IRS2Go specifically. IRS2Go is non-recordkeeping. It is a mobile app used to collect and display public IRS.gov website information to mobile devices. It is not a data repository system. No records scheduling actions for IRS2Go are required. Audit requirements are instead implemented by systems that IRS2Go enables taxpayers to connect with, for example, Where's My Refund.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

IRS2Go is a mobile app, and not a system. Other testing is performed on IRS2Go, including System Acceptance Testing, Application Quality Testing, Section 508 accessibility testing, and cybersecurity testing (SA&A).

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: Not Applicable

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