## 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 Submission:** Sept. 11, 2012 PIA ID Number: **396**

**1. What type of system is this?** New

**1a. Is this a Federal Information Security Management Act (FISMA) reportable system?** No

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

**IRS2Go**

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

**If yes, please state the previous system name, acronym, and release/milestone (if appropriate):**

**3. Identify how many individuals the system contains information on**

| | |
|---|---|
| Number of Employees: | Not Applicable |
| Number of Contractors: | Not Applicable |
| Members of the Public: | Not Applicable |

**4. Responsible Parties:**

N/A

**5. General Business Purpose of System**

irs2go is the first IRS smart phone application for iphones. Mobile application available for iOS devices and Android devices. Allows users to watch videos, sign up for tax tips, check on the status of their refund, order a transcript, contact us, and see the latest news. The app was developed to comply with a White House mandate to create mobile apps for government agencies.

**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

**6a. If Yes, please indicate the date the latest PIA was approved:**

**6b. If Yes, please indicate which of the following changes occurred to require this update.**

- System Change (1 or more of the 9 examples listed in OMB 03–22 applies) (refer to PIA Training Reference Guide for the list of system changes)
- System is undergoing Security Assessment and Authorization

**6c. State any changes that have occurred to the system since the last PIA**

**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'.** NA

## 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

**8a. If No, what types of information does the system collect, display, store, maintain or disseminate?**

**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 | No | |
| | | *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 | No | No | No |
| Social Security Number (SSN) | Yes | Yes | No |
| Tax Payer ID Number (TIN) | No | No | No |
| Address | Yes | Yes | No |
| Date of Birth | Yes | Yes | No |

**Additional Types of PII:** No

No Other PII Records found.

**10a. Briefly describe the PII available in the system referred to in question 10 above.**

The PII in the system is used only for authentication purposes and mirrors the Web application.

**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.)**

IRS2Go retrieves data from the existing web applications that currently operate on the irs.gov website. The same data that taxpayer can currently get by using the irs.gov website.

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

The SSN is masked.

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

SSN is required for certain applications such as where's my refund. IRS could not provide the service without it.

**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 <u>not</u> needed.**

There is no audit trail. IRS2Go is non–recordkeeping. It is a smartphone application 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.

**11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*?** No

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

**a. IRS files and databases:** No

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

No System Records found.

**b. Other federal agency or agencies:** No
If **Yes**, please list the agency (or agencies) below:

**c. State and local agency or agencies:** No
If **Yes**, please list the agency (or agencies) below:

**d. Third party sources:** No
If yes, the third party sources that were used are:

**e. Taxpayers (such as the 1040):** Yes

**f. Employees (such as the I–9):** No

**g. Other:** No If **Yes**, *specify*:

## 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.**

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 information 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 required identification of the user, no personnally identifiable information 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.

## 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 | No | |
| 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

**15a. If yes, with whom will the information be shared? The specific parties are listed below:**

| | Yes/No | Who? | ISA OR MOU**? |
|---|---|---|---|
| Other federal agency (–ies) | | | |
| State and local agency (–ies) | | | |
| Third party sources | | | |
| Other: | | | |

** Inter–agency agreement (ISA) or Memorandum of Understanding (MOU)

**16. Does this system host a website for purposes of interacting with the public?** No

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

If yes, please indicate means:

| | YES/NO | AUTHORITY |
|---|---|---|
| Persistent Cookies | | |
| Web Beacons | | |
| Session Cookies | | |
| Other: | | *If other, specify:* |

## 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?**

yes, they choose to use the services provided, and by doing so, agree to the uses of the information provided such as for 'where's my refund'

**19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?** Not Applicable

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

**20. Did any of the PII provided to this system originate from any IRS issued forms?** No

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

No forms found.

**20b. If No, how was consent granted?**

| | |
|---|---|
| Written consent | No |
| Website Opt In or Out option | Yes |
| Published System of Records Notice in the Federal Register | No |
| Other: | No |

## 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:** IRS Owned and Operated

**21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?**

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

| | Yes/No | Access Level |
|---|---|---|
| IRS Employees: | No | |
| Users | | No Access |
| Managers | | No Access |
| System Administrators | | |
| Developers | | |

| | | |
|---|---|---|
| Contractors: | No | |
| Contractor Users | | |
| Contractor System Administrators | | |
| Contractor Developers | | |
| Other: | No | |

**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?**

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

Taxpayer is already able to access the same data and services by visiting IRS.Gov. The irs2go application for iphones uses the same data to display them in the mobile systems.

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

Tax data is verified using the same existing verification processes that the IRS uses on the Web applications for "Where's my Refund" and "Order a Transcript"

**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 Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.**

**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.**

IRS2Go is non–recordkeeping. It is a smartphone application 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.

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

The application data is already synched with the API As the user enters their SSN it is masked and the application doesn't retain the data.

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

The data is passed through the API. Dorothy comment – need a more complete answer to this question. what measures does MITS take to ensure that the information is not stolen in flight or in transition? if they have no measure, explain why not needed or why it can't be done.

**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.**

This is not applicable to a mobile application. The secure applications are monitored via the Web version of the application on the RUP.

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 – *IT Security, Live Data Protection Policy*?** Not Applicable

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*?**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?**

## 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.**

## 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 | No |
| New privacy measures have been considered/implemented | No |
| Other: | No |

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

N/A

**View other PIAs on IRS.gov**