

NOTE: The following reflects the information entered in the PIAMS website.

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: June 10, 2014

PIA ID Number: **880**

1. What type of system is this? Non-Major System

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

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

Personal Global Positioning Systems, GPS

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: 100,000 - 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The purpose of the Global Positioning System (GPS) is to assist IRS employees in locating persons with whom they have official business. The GPS device provides built-in capabilities that simplify the navigation process. The benefits of using this device are as follows: • Reduces government cost • Increase field time efficiency with preloaded detailed maps • Increase employee safety with text-to-speech capability, allowing drivers to keep their eyes on the road while receiving voice prompt directions • Reduce time spent mapping for field visits • Basic GPS units have rerouting capability • Automatically plots the most direct routes when multiple stops are input • Allow for programming multiple stops and rerouting when new address is located • Reduce cost of paper for printing and purchasing map books The GPS will be a stand-alone device where employees will manually enter the destination location and the navigational information will be transmitted to the system via satellite. The GPS information will not be used to adversely affect an employee's performance evaluation.

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) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 11/23/2010

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) No
 - System is undergoing Security Assessment and Authorization No
-

6c. State any changes that have occurred to the system since the last PIA
none

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	<u>No</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>Yes</u>	<u>Other Source:</u> <u>Navigation satellite</u>

-
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)	No	No	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	Yes
Date of Birth	No	No	No

Additional Types of PII: No

No Other PII Records found.

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

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.)

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

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

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

A. Taxpayer Manual input to device to determine directions to the location of an individual or business taxpayer. Employees will be instructed only to input the address data. No taxpayer or business entity will be permitted to be entered into the GPS device. B. Employee Manual input to device of personal and/or business address to return from field location. C. Audit Trail Information No audit trail of locations entered and visited. Guidelines will be provided to employees pertaining to the storage and deletion of locations entered into GPS device.

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.

No audit trail of locations entered and visited. Employees may only enter the taxpayer's address into the device. Guidelines were provided to employees pertaining to the storage and deletion of locations entered into GPS device. There is no "log-in" feature. The unit is ready to use when turned on.

- 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: Yes

If **Yes**, please list the agency (or agencies) below:

Federal/State/Local Agencies (e.g. Postal Service)

c. State and local agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

Uniformed Commercial Code, DMV, etc.

d. Third party sources: Yes

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

3rd party sources (e.g. neighbors/employers)

e. Taxpayers (such as the 1040): Yes

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

g. Other: Yes If **Yes**, *specify*: Employees will be working open Individual and Business delinquent cases within their designated caseload. The data is obtained from the case file, which is gathered from IRS systems, 3rd party sources (e.g. neighbors/employers) and Federal/State/Local Agencies (e.g. Postal Service, Uniformed Commercial Code, DMV, etc.) The system is a stand-alone device that will not receive or send information to or from any IRS or outside systems, only satellite.

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.

To simplify Navigation in unfamiliar settings for compliance personnel conducting field investigations and enforcement activities.

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	<u>Yes</u>
To provide taxpayer services	<u>No</u>
To collect demographic data	<u>No</u>
For employee purposes	<u>Yes</u>

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? 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	_____	_____

If other, specify:

Other: _____

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? Not Applicable

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

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

20. Did any of the PII provided to this system originate from any IRS issued forms? 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:	<u>Yes</u>	

Users		Read Only
Managers		Read Only
System Administrators		No Access
Developers		No Access
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?

Employees such as field agents who have a specific need to know this information will have access to the data. It will be used to locate taxpayers with whom the IRS has official business. At the time of the GPS Project in 2009, the Business Reengineering operating unit in Headquarters was under the Collection Operating Unit and set the policy for GPS usage by Collection personnel. Employees such as field agents who have a specific need to know this information will have access to the data. Guidelines were developed outlining the proper usage, security requirements, and restrictions for using the device. These guidelines were in accordance with the applicable IRMs pertaining to PII and personal use. The devices are also used by management, executive and field analysts to aid in navigation for POD visits, meetings, etc.

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

The GPS is a stand-alone device where employees manually enter the destination location and the navigational information is transmitted to the system via satellite. Employee feedback was used to inform management of how well the device provides accurate and timely information. There is no IT or technical support provided by the IRS for these personal devices. There will be no mapping software updates to the devices and no model upgrades. Once the devices are no longer operable, they will not be replaced.

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.

The Personal Global Positioning System (GPS) is non-recordkeeping, and requires no records scheduling actions. GPS users follow the same guidance issued to Criminal Investigation employees in Memorandum titled Criminal Investigation Security Policy on Portable Storage Devices (PSD) dated May 20, 2009, based on IRM 2.14 and 10.8.1 in the handling of the GPS device, as well as the storage and deletion of locations entered into the device. Employees have the ability to save location data and determine when the location data should be deleted from the GPS device.

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

Employees work open Individual and Business delinquent cases within their designated caseload. The data is obtained from the case file, which is gathered from IRS systems, 3rd party sources (e.g. neighbors/employers) and Federal/State/Local Agencies (e.g. Postal Service, Uniformed Commercial Code, DMV, etc.) The system is a stand-alone device that will not receive or send information to or from any IRS or outside systems, only satellite. The GPS will automatically plot the best route for employees to follow. The data retrieved will be used to locate the addresses

of tax payers for which the IRS has official business. The address is the only piece of information being used to identify taxpayers. There will be no other unique identifiers transmitted within the device. The device will not be used to track employees and the address information will be erased from the device when it is no longer needed. Employees are subject to current IRS policies regarding the protection of PII.

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

Employees should take every precaution to prevent the GPS device from being left unattended or unsecured. Devices should be removed from vehicles when not in use as circumstances permit. In those limited instances where a device is left in a locked vehicle, it should be stored out of sight in the trunk or glove compartment. Devices should never be left in vehicles overnight. The device and any mounts should not be left in an unattended vehicle in plain sight. The suction cup mount area should be wiped clean because it can leave marks on the windshield/dashboard indicating that a GPS or other device may be present in the vehicle, increasing the risk of a break-in. Only taxpayer address information may be input into the GPS device, and this information must be deleted from the device once it is no longer necessary. Individual or business taxpayer names should never be input into the device. A security PIN code must be used with the device to help protect the privacy of taxpayer information in the event the device is lost or stolen. The GPS device may not be connected to an IRS computer as the device has the potential to introduce computer viruses and malware into the IRS network. As with all IRS-issued equipment, the GPS device may not be connected to a non-IRS computer since it may contain taxpayer information. No personal files or software may be added to the device.

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.

If a GPS device is lost or stolen, the employee responsible for the device must immediately notify his/her manager, as well as, the Computer Security Incident Response Center (CSIRC 866-216-4809) and the Treasury Inspector General for Tax Administration (TIGTA 800-366-4484) to report the loss/theft.

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

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? No

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) No

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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

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

NA