Date of Approval: 10/23/2017 PIA ID Number: **2884**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Wi-Fi Tools for Analysis and GEO Locating Program, WTAG

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No ___ Vision & Strategy/Milestone 0
No ___ Project Initiation/Milestone 1
No ___ Domain Architecture/Milestone 2
No ___ Preliminary Design/Milestone 3
No ___ Detailed Design/Milestone 4A
No ___ System Development/Milestone 4B
No ___ System Deployment/Milestone 5
Yes __ Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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. Internal Revenue Service Criminal Investigation (IRS-CI) has purchased a Wi-Fi tool (WTAG) that allows special agents to locate wireless electronic devices that emit a Wi-Fi signal. This handheld device captures the Media Access Control (MAC) address of any Wi-Fi device that is within Wi-Fi range, and can provide geolocation of the device. Special Agents will only be permitted to use this electronic device during the execution of a validly authorized search warrant. The affidavit in support of the search warrant must set forth probable cause to believe electronic devices will be found at the premises to be searched and will contain evidence of the alleged criminal activity. Furthermore, the affidavit must include a computer search protocol that specifies that a Wi-Fi surveillance device will be used. Overall, this Wi-Fi tool will assist special agents with potentially finding hidden electronic devices that emit a Wi-Fi signal and may have been used in furtherance of a crime. The geolocation feature of the WTAG device will only take place in the area outlined in the search warrant.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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.)? No

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays,

stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Media Access Control (MAC) address - it is a globally unique identifier assigned to network devices, and therefore it is often referred to as the hardware or physical address.

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(
No	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
Yes	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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 the criteria. Be specific. IRS-CI uses WTAG to locate potential electronic devices used in furtherance of a crime. When deployed, IRS-CI's WTAG device captures the Media Access Control (MAC) address of any Wi-Fi device that is within Wi-Fi range, and can provide geolocation of the device. The systems are only deployed during the execution of a validly authorized search warrant. The affidavit in support of the search warrant must set forth probable cause to believe electronic devices will be found at the premises to be searched and will contain evidence of the alleged criminal activity. Furthermore, the affidavit must include a computer search protocol that specifies that a Wi-Fi surveillance device will be used.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. IRS will ensure an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. IRS-CI has a draft policy in place that will be issued soon. This policy requires a validly authorized search warrant. The affidavit in support of the search warrant must set forth probable cause to believe electronic devices will be found at the premises to be searched and will contain evidence of the alleged criminal activity. Furthermore, the affidavit must include a computer search protocol that specifies that a Wi-Fi surveillance device will be used. As mentioned, the device only performs geolocation of a specific MAC address. The device does not store, maintain, or disseminate this information. Once the device is turned off, all MAC addresses gathered are automatically deleted.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
Treas/IRS 46.005	IRS 46.005--Electronic Surveillance and Monitoring

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources. The information is not collected directly from the individual. The information is collected from any electronic device which emits a Wi-FI signal. The WTAG device is used to find these devices in the case they are hidden in ceilings, behind walls, or other areas. As indicated, a search warrant will be required to use this device.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? Government agents using the device will have a valid search warrant for the use of the device

19. How does the system or business process ensure due process regarding information access, correction and redress? IRS-CI will have a formal policy in place prior to authorizing the use of the WTAG device. This policy will require a valid search warrant be in place prior to deploying the WTAG device.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Administrator
Managers	No	
Sys. Administrators	No	
Developers	No	

21a. How is access to SBU/PII determined and by whom? A search warrant must be obtained to use the WTAG device. The operation of the WTAG device is relatively complex and all Users must have completed training at the Federal Law Enforcement Training Center. The system operators are the only individuals that would have access to MAC addresses while the unit is in search mode.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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? Yes

22a. 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.

The search warrant will disclose the use of the WTAG system. After case completion, the case file will be managed according to requirements under IRM 1.15.1 and will be scheduled as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. IRS CI Investigative Case Files and Related Records are scheduled under IRS RCS 30, Item 15.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system s audit trail. The systems are purchased and shipped to each field office. The equipment is maintained in the field office's tech agent's inventory. Upon search warrant approval, the equipment is then deployed and assists in locating hidden electronic devices that may be emitting a wi-fi signal. Upon completion of the search warrant, the equipment is returned to the tech agent's inventory. A copy of the search warrant is maintained in the case file and will be stored per IRM 1.15.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. The WTAG system is only deployed upon approval of a valid search warrant. The system is used to identify hidden devices within the search parameters. Upon completion of the operation, the unit is turned off and all MAC addresses obtained are deleted.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000). The number of MAC addresses will be based on the number of wi-fi devices turned on in the surrounding area. However, the user of the device will only attempt to locate those devices with the strongest signal, as the weaker signals will be outside the search warrant area. In a populated residential area, there is a potential of capturing 50 MAC addresses.

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

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

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. There are privacy controls and 4th amendment controls in that CI recognizes that this is a fourth amendment search and a search warrant is required by CI policy. A search warrant is required and there are constitutionally guaranteed due processes for criminal suspects.

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report