
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. CI Use of Stingray II, Stingray II

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

CI Use of Stingray II, Stingray II, 1572

Next, enter the **date** of the most recent PIA. 4/8/2016

Indicate which of the following changes occurred to require this update (check all that apply).

- No Addition of PII
- No Conversions
- No Anonymous to Non-Anonymous
- No Significant System Management Changes
- No Significant Merging with Another System
- No New Access by IRS employees or Members of the Public
- No Addition of Commercial Data / Sources
- No New Interagency Use
- No Internal Flow or Collection

Were there other system changes not listed above? Yes

If yes, explain what changes were made. Changes to information contained in sections #14, and #29.

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.

In September 2011, Internal Revenue Service Criminal Investigation (IRS-CI) procured a Stingray II cell-site simulator. The cell-site simulator receives and uses an industry-standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular device. By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is, however limited. Cell-site simulators only provide the relative signal strength and general direction of the subject cellular device; they do not function as a Global Positioning System (GPS) locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by IRS-CI must be configured as pen registers and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the device itself. The simulator does not remotely capture voice communication, emails, texts, contact lists, images or any other content data from the device. Moreover, cell-site simulators used by IRS-CI do not provide subscriber account information (for example, an account holder's name, address, or telephone number). The range of the cell-site simulator varies by geography and topography. For example, radio signals will travel much farther in a rural versus urban setting. The Stingray II does not have the ability to conduct Title III (Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a/k/a Wiretap Act 18 U.S.C. §§ 2510-22, as amended by the Electronic Communications Privacy Act) phone taps or receive any content such as email, voice, or text. In November 2012, IRS-CI purchased the Hailstorm upgrade for its Stingray II cell site simulator. The Hailstorm upgrade provides an additional two channels of monitoring that allows IRS-CI to target 4G phones/LTE devices. Regarding the use of a Stingray II cell site simulator, in the absence of qualifying exigent circumstances, IRS-CI must first obtain a court order to obtain the geolocation and cellular device number, either the Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI), or the International Mobile Station Equipment Identifier (IMEI), from the phone company. Upon obtaining the cellular device number and geolocation information from the phone company and after a search warrant is obtained, the cell-site simulator is taken to the area where the known cellular device is being used. The cell-site simulator then begins tracking the device via signal strength, and points the user in the direction where the device is currently located. While in operation, the cell-site simulator builds a database of the device identification numbers it finds while in search mode. The IRS-CI Policy Memorandum dated November 30, 2015, regarding the use of cell-site stimulator technology, mirrors the guidelines set by the Department of Justice to ensure the protection of privacy and civil liberties of the public. Therefore, IRS-CI only obtains a device I.D. number and geolocation from the phone company after first obtaining a court order. The phone company will not release the device I.D. and geolocation without a court order. The IRS-CI policy requires a search warrant to use the Stingray II to search for the device I.D. If IRS-CI obtains the warrant, the device I.D. is then tracked using the Stingray II. As a practical matter, because agents/operators, in consultation with prosecutors, will need to seek authority pursuant to Rule 41 and the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the section of the IRS-CI policy titled ("Applications for Use of Cell Site Simulators"). There is one circumstance in which this policy does not require a warrant prior to the use of a cell-site simulator. These are exigent circumstances under the Fourth Amendment; this exception mirrors current Department of Justice policy.

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

If **yes**, check who the SSN (or tax identification number) is collected on.

No On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

No Social Security Number (SSN)
No Employer Identification Number (EIN)
No Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Practitioner Tax Identification Number (PTIN)

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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	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	Information concerning IRS criminal investigations or the

Investigation agents conducting the investigations.
Information

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. The Stingray II captures device identification numbers which is PII because it's linkable to an individual. IRS-CI policy requires IRS-CI to delete all device identification numbers captured at the end of an operation. IRS-CI uses evidence obtained on an individual target and the device they use in getting a court order for the "device I.D." from the phone company. The device I.D. is then tracked via a search warrant using the Stingray II.

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

<u>No</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>Yes</u>	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 this criteria. Be specific.

IRS's use of the cell-site simulator technology is limited strictly to IRS Criminal Investigation, the law enforcement arm of the Internal Revenue Service. The cell-site simulator technology is a law enforcement tool that only trained law enforcement agents have used in carrying out criminal investigations in accordance with all appropriate federal and state judicial procedures. IRS-CI has used the cell-site simulator in support of grand jury investigations, led by the Department of Justice, into allegations of stolen identity fraud and money laundering violations. The technology IRS-CI owns cannot be used to intercept the content of real-time communications, including phone calls, text messages, or emails. Rather, IRS-CI uses it only to identify the location of a specific mobile cellular device. IRS-CI has used the cell-site simulator to assist federal, state and local law enforcement agencies in on-going IRS-CI investigations. On each occasion, IRS-CI operated the cell-site simulator, worked under the direction of a prosecutor, and followed all applicable laws. All device identification numbers that were collected through the system were deleted at the completion of the operation.

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-CI works with the United States Attorney's Office (USAO) or state prosecutor in obtaining the required approved Pen Register/Court order to obtain cellular device identification numbers and geolocation. Once the cellular device identification numbers and geolocation are obtained, IRS-CI,

continuing to work with the USAO or state prosecutor, obtains the required search warrant to operate the Stingray II to collect identifying numbers from cellular devices within a geographical range in order to find and track a specific cellular identifying number. Aside from the known targeted cellular device, IRS-CI does not determine the number of cellular devices whose data is captured during the agency's use of a cell site simulator. IRS-CI personnel delete all non-target cellular device information that is gathered daily. IRS-CI is committed to ensuring that its law enforcement practices concerning the collection or retention of data are lawful and respect the important privacy interests of individuals. As part of this commitment, IRS-CI operates in accordance with rules, policies and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, IRS-CI's use of cell-site simulators includes the following practices: 1). When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located and no less the once daily. 2). Prior to deploying equipment for another mission, the agent/operator must verify that the equipment has been cleared of any previous operational data. 3). IRS-CI ensures that the data is deleted in the manner described above. Standard operating procedures will address the specifics of the audit conducted by special investigative techniques program analysts during the Annual Sensitive Review. It should be noted that IRS-CI does not share data collected from the cell-site simulator, however, IRS-CI does work closely with other federal, state and local law enforcement partners and provides technological assistance under a variety of circumstances, such as in joint federal grand jury investigations.

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

IRS 46.005

Electronic Surveillance and Monitoring Records

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. ## Redacted Information For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
--------------------------	----------------------------	----------------

Cellular phone company	Manually input	No
------------------------	----------------	----

Cellular devices	Cell site simulator	No
------------------	---------------------	----

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? 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, cloud, global position system (GPS), biometrics, RFID, etc.? Yes

14a. If **yes**, briefly explain how the system uses the referenced technology. As explained in question 5, the Stingray II with the Hailstorm upgrade allows it to look at 6 channels of cellular transmissions (two of which are 4G/LTE). If the target device is located within these six channels, it will begin tracking the device based on the device's signal strength.

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 needed (a device identification number and geolocation) is obtained through a court order. The Stingray II is then used in a covert manner to find the device, as there is probable cause showing the device is associated with money laundering, identity theft, or other criminal activity.

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? As noted above, the information needed (a device identification number and geolocation) is obtained through a court order. The Stingray II is then used in a covert manner to find the device, as there is probable cause showing the device is associated with money laundering, identity theft, or other criminal activity.

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

IRS-CI has a formal policy and procedures for the Stingray that follows Department of Justice guidelines for cell-site simulator technology. Most importantly, IRS-CI requires a search warrant in order to track a device identification. IRS-CI has a formal policy and procedures for the Stingray that follows Department of Justice guidelines for cell-site simulator technology. Most importantly, IRS-CI requires a search warrant in order to track a device identification number. Without a search warrant IRS-CI is not allowed to use the Stingray II for device tracking. Furthermore, IRS-CI requires all device I.D. numbers collected by the Stingray, in its search for the targeted device, to be deleted at the end of the operation. In addition, IRS-CI requires a log to be maintained. This log contains the date of the operation, the case name and number, the start and end time, and the date the data was deleted. Otherwise, statutory criminal due process applies.

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

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

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The use of a cell-site simulator by IRS-CI must be approved by a Special Agent in Charge (SAC). IRS-CI personnel must be trained and supervised appropriately. When Stingray II is used for grand jury investigations (Title 18 and Stolen Identity Refund Fraud), evidence in a case brought before the grand jury may only

be disclosed in accordance with Federal Rule of Criminal Procedure 6(e), which restricts access to information related to grand jury matters to those individuals who have a "particularized need" for the materials. This includes the individuals operating the Stingray II in search of the device I.D. obtained via a court order. As noted previously, the Stingray cannot be used without first obtaining a search warrant.

- 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? No

- 22b. 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.

Data from the Stingray is purged after completion of the operation. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system, or developed in conjunction with the use of the system (i.e. Cell Site Simulator Log), will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be scheduled as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data. The Special Agent in Charge (SAC) or his/her designee shall audit the cell-site simulator log assigned to their office to ensure that the data is deleted in the manner described above. Special Investigative Techniques Program Analysts will verify that audits have been conducted during the Annual Sensitive Review. In addition, per Standard Operating Procedures dated January 12, 2016, the SAC will maintain a log for their assigned cell site simulator that identifies the following: The usage reflecting the total number of times a cell-site simulator is deployed in the jurisdiction and the number of times the technology is deployed in emergency circumstances.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. Per Department of Justice (DOJ) guidelines, the Stingray II can only be used after obtaining a search warrant. In addition, all information is deleted at the end of the operation.

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: Under 100,000
26d. Other: No

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. IRS-CI seeks to obtain information after obtaining legal permission through a warrant or under qualifying exigent circumstances following Department of Justice guidelines and accepted jurisprudence. The cell-site simulator receives and uses an industry-standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular device. By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is, however limited. Cell-site simulators only provide the relative signal strength and general direction of the subject cellular device; they do not function as a GPS locator, as they do not obtain or download any location information from the device or it's applications. Moreover, cell-site simulators used by IRS-CI must be configured as pen registers and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the device itself. The simulator does not remotely capture voice communication, emails, texts, contact lists, images or any other content data from the device. Moreover, cell-site simulators used by IRS-CI do not provide subscriber account information (for example, an account holder's name, address, or telephone number). The range of the cell-site simulator varies by geography and topography. For example, radio signals will travel much farther in a rural versus urban setting. Regarding the use of a Stingray II cell site

simulator, in the absence of qualifying exigent circumstances, IRS-CI must first obtain a court order to obtain the geolocation and device number, either the Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI), or the International Mobile Station Equipment Identifier (IMEI), from the phone company. Upon obtaining the device number and geo-location from the phone company and after a search warrant is obtained, the Stingray II is taken to the area where the cellular device is being used. The Stingray II then begins tracking the device via signal strength, as it points the user in the direction where the device is located. While in operation, the Stingray II builds a database of the device identification numbers it finds. The Stingray II is used by IRS-CI for criminal investigations involving Title 18 charges (Money Laundering & Identity Theft). IRS-CI uses evidence obtained on an individual target and their device when seeking a court order and search warrant. At the end of the operation, the database of identification numbers is deleted. The deletion of all device identification numbers at the end of an operation is required by IRS-CI policy.

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
