Date of Approval: June 16, 2016 PIA ID Number: **1732**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. IP Camera Systems, IP Camera

2. Is this a new system? No

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

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

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.

IRS-CI currently operates covert video surveillance systems to enhance the surveillance capabilities of special agents in ongoing criminal investigations. Surveillance situations are numerous, but include identifying individuals and/or vehicles coming and going into a residence or

business. The surveillance video is used to potentially establish probable cause for a search warrant and/or obtain additional evidence for a potential criminal prosecution. Overall, the video surveillance is used to build evidence against an alleged individual associated with money laundering, identity theft, and/or other criminal activity. Prior to 2008, these video surveillance systems were composed primarily of surveillance vans and other small, short-term surveillance cameras which required on-site monitoring. In 2008, IRS-CI received initial funding for its inventory of Internet Protocol (IP) Cameras or "pole cameras." Pole cameras get their name from the first generation of IP cameras, which were designed to be mounted on utility poles and street lights. While many are still designed this way, newer devices come in many configurations (containers) that are designed to blend in with the deployment environment. However, the term "pole cam" is still in use to refer to IP cameras in general. These cameras offer additional capabilities, including persistent deployment, off-site data storage, increased recording capability, and remote access and viewing. This last feature is of particular note: prior to the IP Cameras, an agent had to be in close proximity to a recording device to be able to view the video stream live or to retrieve the stored video. These systems free up a tremendous amount of agent man-hours and are safer for agents in areas where surveillance is difficult. IP cameras transmit through cellular networks to the internet to stream live video surveillance. On the receiving end, IRS-CI uses a network video recorder (NVR) which can archive the video to any standard storage media, such as thumb drives or external hard drives

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.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
No	Name	No	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No

No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	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	Information concerning IRS criminal investigations or the

Investigation Information	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. Depending on the surveillance, IRS-CI's IP Camera system can capture vehicle license plate information.

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

No	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a
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

If the answer to 6f is **No**, verify the authority is correct with the system owner and then update the answer to 6f.

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.

IP cameras are used in conducting video surveillance to build evidence in investigations of alleged criminal activity associated with money laundering, identity theft and other financial crime. The use of IP camera to observe activity that is viewable by the public, either because members of the public can lawfully access the area where this activity occurs or can see the activity from a lawful vantage point, does not generally constitute an intrusion into a constitutionally protected private interest. A warrant is generally not required to visually record activities that occur in publicly accessible areas such as public parks, sidewalks, streets, open fields, and other areas outside the curtilage of a house that is not commonly accessible to the public. The Fourth Amendment does not require law enforcement officers to shield their eyes when passing a home on a public thoroughfare. Officers may, without a search warrant, use video surveillance to assist them in observing certain areas even when the areas are within the curtilage of a house if others can observe these same areas from a place they are lawfully entitled to be (i.e., from the street, sidewalk, or an open field). This would include unobstructed video surveillance of driveways, front doorways, and yards of businesses or houses. IRS-CI records its IP cameras using a network video recorder. Upon completion of the recording, the storage media is maintained by the evidence custodian. . IRS-CI follows the Fourth Amendment guidelines on the use of IP cameras. IRS-CI Standard Operating Procedures (SOP) are more conservative than required by law. Under the Fourth Amendment, US vs Katz, expectation of privacy is protected by a reasonableness standard. The law clearly states that areas in public view do not meet this standard

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 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 an IP Camera system. It should be noted that IRS-CI does not share data collected from its IP Camera systems, 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. IRS-CI's policy ensures individual right's are not violated, as IP camera system deployments must obtain the appropriate authorization and can't exceed specific time limits outlined in its policy.

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? 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.? 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 video surveillance is used to build evidence against an alleged individual associated with money laundering, identity theft, and/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? The video surveillance is used in a cover manner to assist IRS-CI develop probable cause for a search warrant or establish additional evidence of criminal activity.

19. How does the system or business process ensure due process regarding information access, correction and redress?
IRS-CI follows all applicable laws and follows internal policy when conducting video surveillance of public view areas. IRS-CI's internal policy requires Special Agent in Charge approval for surveillance activities 30 days or less. For surveillance activities extending 31 days to 90 days, Special Agent in Charge approval and Criminal Tax Counsel (CT) review is needed. For surveillance extending beyond 90 days, Director of Field Operations (DFO) and Special Agent in Charge approval is required in addition to Criminal Tax review. The initial request for use is always 30 days. During the first 30 days, there must be written justification to extend the video surveillance beyond the initial 30 days.

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	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 the IP Video Surveillance camera must be approved by the Special Agent in Charge. Deployments lasting longer than 30 days require Criminal Tax review in addition to Special Agent in Charge approval. Deployments lasting longer than 90 days, must obtain the Director of Field Operations and Special Agent in Charge approval and Criminal Tax Review. The initial request for use is always 30 days. During the first 30 days, there must be written justification to extend the video surveillance beyond the initial 30 days. As indicated, the video collection is archived to electronic storage media. The storage media is maintained with the evidence custodian. The video is generally reviewed by the case agent to determine if it provides any value to establishing additional evidentiary facts for the case. Upon completion of the criminal case, the electronic storage media will be maintained as mandated by the Federal Records Center.

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.

All IPCamera video surveillance records will be destroyed at the conclusion of their retention period(s) as required under IRM 1.15.6 and approved retention periods. These are the official records and have National Archives approval to affect data disposition. These records will be managed according to requirements of the IRS Records Control Schedule (RCS) 30, Part II, Item 15, and 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. The systems are purchased and shipped to each field office. The equipment is maintained in the field office's tech agent's inventory. Upon SAC approval, the equipment is then deployed as approval permits (30, 60, 90 days). Upon completion of the deployment, the equipment is returned to the tech agent's inventory. The storage media which collected the video surveillance is maintained by the evidence custodian and is reviewed by the case agent. Upon closure of the criminal case, the storage media is managed according to IRM 1.15.6.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. IP Camera surveillance is deployed via SAC approval. The digital media capturing the video surveillance is maintained by an evidence custodian. Upon conclusion of the criminal case, the storage media is managed according to IRM 1.15.6.

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: More than 1,000,000
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? Yes

27a. If **yes**, explain the First Amendment information being collected and how it is used. In certain situations, the IP surveillance camera may capture individuals or groups of people that are not connected to criminal activity. Use of a video camera or IP camera (pole cameras) to observe activity that is viewable by the public (either because members of the public can lawfully access the area where this activity occurs or can see the activity from a lawful vantage point) does not generally constitute an intrusion into a constitutionally protected private interest. A warrant is generally not required to visually record activities that occur in publicly accessible areas such as public parks, sidewalks, streets, open fields, and other areas outside the curtilage of a house that is not commonly accessible to the public. However, IRS-CI requires a search warrant pursuant to 18 USC §3102 and Rule 41(a) of the Federal Rules of Criminal Procedure (Fed. R. Crim. P.) when obtaining evidence that cannot be observed from a public place with the un-aided eye. As indicated, IRS-CI's IP surveillance cameras are used for situations that require long-term surveillance and would result in a significant amount of human resource hours or in situations where it is not safe to conduct a human surveillance. Surveillance situations are numerous, but include identifying individuals and/or vehicles coming and going into a residence or business. The surveillance video is used to potentially establish probable cause for a search warrant and/or obtain additional evidence for a potential criminal prosecution.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). No
The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q 7) Yes
There is a statute that expressly authorizes its collection. (Identified in Q6) Yes

27c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges? 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. In certain situations, the IP surveillance camera may capture individuals or groups of people that are not connected to criminal activity. Use of a video camera or IP camera (pole cameras) to observe activity that is viewable by the public (either because members of the public can lawfully access the area where this activity occurs or can see the activity from a lawful vantage point) does not generally constitute an intrusion into a constitutionally protected private interest. A warrant is generally not required to visually record activities that occur in publicly accessible areas such as public parks, sidewalks, streets, open fields, and other areas outside the curtilage of a house that is not commonly accessible to the public. However, IRS-CI requires a search warrant pursuant to 18 USC §3102 and Rule 41(a) of the Federal Rules of Criminal Procedure (Fed. R. Crim. P.) when obtaining evidence that cannot be observed from a public place with the un-aided eye. As indicated, IRS-CI's IP surveillance cameras are used for situations that require long-term surveillance and would result in a significant amount of human resource hours or in situations where it is not safe to conduct a human surveillance. Surveillance situations are numerous, but include identifying individuals and/or vehicles coming and going into a residence or business. The surveillance video is used to potentially establish probable cause for a search warrant and/or obtain additional evidence for a potential criminal prosecution.

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