Date of Approval: **December 13, 2019**

PIA ID Number: **4551**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

IP Camera System, IP Camera

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

IP Camera Systems, IP Camera, PIA ID Number: 1732

What is the approval date of the most recent PCLIA?

5/24/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

N/A

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

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, tax crimes and/or other criminal activity under the jurisdiction of IRS-CI. 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 gov-cloud hosted servers and software which can archive the video and allows for the transfer of video to any standard storage media.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Vehicle Identifiers

Photographic Identifiers

Biometric Identifiers

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

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

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Depending on the specific circumstances, IRS-CI's IP Camera system can capture vehicle license plate information and photographic identifiers.

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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, criminal tax, 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 specialized hardware and software. 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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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. 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 rights are not violated, as IP camera system deployments must obtain the appropriate authorization and can't exceed specific time limits outlined in its policy. Criminal Tax Counsel reviews all IP Camera uses beyond 30 days.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 46.005 Electronic Surveillance and Monitoring Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified {MM/DD/YYYY}

5/1/2013

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

None

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage

Transmission

Maintenance

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

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, criminal tax and/or other criminal activity.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The video surveillance is used in a covert manner to assist IRS-CI develop probable cause for a search warrant, establish additional evidence of criminal activity, and gather information prior to an enforcement action for officer safety.

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 Supervisory Special Agent approval for surveillance 5 day or less, 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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Only

Managers: Read Write

System Administrators: Administrator

How is access to SBU/PII determined and by whom?

The use of the IP Video Surveillance camera must be approved by a Supervisory Special Agent for up to five days and the Special Agent in Charge for longer deployments. 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. 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 in the cloud and/or storage media. 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

System access is controlled by written request and access is limited based on user permissions. Written approval from the Special Agent in Charge are required for equipment deployment 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.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

IP Camera surveillance is deployed via Special Agent in Charge 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.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

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 Â§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.

Please list all exceptions (any one of which allows the maintenance of such information) that apply:

The information maintained is pertinent to and within the scope of an authorized law enforcement activity (as noted in Q 7).

There is a statute that expressly authorizes its collection (identified in Q6).

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

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

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 Â§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.

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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