Date of Approval: 11/03/2025
Questionnaire Number: 2683

# Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?
> IP Camera System

Business Unit
> Criminal Investigation

Preparer
> # For Official Use Only

Subject Matter Expert
> # For Official Use Only

Program Manager
> # For Official Use Only

Designated Executive Representative
> # For Official Use Only

Executive Sponsor
> # For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.
> The IP Camera System is an IRS-Criminal Investigation (CI) law enforcement tool to support criminal investigations and undercover operations. IRS-CI owns and operates the IP Camera System and is hosted in the GOV cloud environment. The IP Camera System is used real-time monitoring and evidence collection of approved criminal investigations. The system may also provide relevant information for officer safety in enforcement, undercover operations, and other criminal investigation activities. The IP Camera System is used by IRS-CI special agents and investigative analysts. The IP Camera System allows IRS-CI to conduct surveillance and obtain evidence in conducting criminal investigations while reducing the time and labored required to plan, conduct, and document the investigative actions. The system provides valuable information special agents to make relevant and timely investigative decisions.

# Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?
> Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).
> The Internet Protocol (IP) Camera System is used to observe activity that is viewable by the public to gather evidence of the alleged criminal activity associated with the bank secrecy act, criminal tax violations, money laundering, identity theft, and other financial crimes. Under the Fourth Amendment, 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). IRS-Criminal Investigation (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 Standard Operating Procedures (SOP) are more conservative than required by law. 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 during any investigation, these authorities apply to information collected using 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.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.
> Photograph
> Vehicle Identification Number (VIN)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
> Information by CI for certain money laundering cases - 18 USC
> PII about individuals for Bank Secrecy Act compliance - 31 USC
> PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

# Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?
>      No

1.1 What is the name of the Business Unit (BU) or Agency initiative?
>      Criminal Investigation

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
>      System

3 What Tier designation has been applied to your system? (Number)
>      Low

4 Is this a new system?
>      No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
>      Yes

4.11 What is the previous PCLIA number?
>      7269

4.12 What is the previous PCLIA title (system name)?
>      IP Camera System, IP Camera

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)
>      Expiring PCLIA. No system changes.

5 Is this system considered a child system/application to another (parent) system?
>      No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.
>      Execution

7 Is this a change resulting from the OneSDLC process?
>      No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

    No

10 Does this system disclose any PII to any third party outside the IRS?

    No

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

    Yes

11.1 Describe the business process and purpose of your Artificial Intelligence (AI) and identify what system(s) or business process(es) this AI supports.

    The IP Camera System includes a commercial off the shelf (COTS) video analytic program that can classify and search objects in the video files with user-controlled confidence level. The video analytics provide of summary list of the objects detected to facilitate the review of voluminous amounts of the video files. Objects are limited to face, person, vehicle, colors, and direction of movement within a confidence level.

11.2 What is the algorithm or learning method used and what database is training your AI?

    Vendor proprietary. Commercial off the shelf (COTS).

11.3 How is this AI system tested and validated to ensure that the decisions or outputs are reliable (relevant to the input) and performs without biases and drifting? Note: Outputs include, User information, transfer to assistor, reports on dashboard depicting activities.

    Outputs were tested against video files with known results. The AI only used to help reduce the review time of video files by detecting objects. Users can control the confidence levels of the object detection.

12 Does this system use cloud computing?

    Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

    AWS, 05/01/2013

12.2 Does the CSP allow auditing?

    Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

    IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).
>   Low

13 Does this system/application interact with the public?
>   No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)
>   The system is only used in support of criminal investigations.

15 Is this system owned and/or operated by a contractor?
>   No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)
>   IRS Roles:
>   System Administrator - Access to the full system.
>   Tech Agents - Access to the management system - may add users and viewing permissions. Can view but does not have direct access to underlying data.
>   Special Agents - Access to limited to approved cameras and time periods (view only roles).

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.
>   IRS 46.005 Electronic Surveillance and Monitoring Records

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".
>   Not Applicable

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".
>   Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".
>   Not Applicable

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

Business Entitlement Access Request System (BEARS) is used to manage access to the IRS-CI TaLON network. The IP Camera System may be accessed through the IRS-CI TaLON network or an app on an IRS-CI managed mobile device. Users are provisioned system access by system administrators based on written management approval. Users are provided read only access to specific devices for the approved time. IRS-CI has a policy in-place specifying the authorized management approval level needed based on the surveillance period.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

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. 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. The system had the ability to block or mask any areas of the video that an individual would have a reasonable expectation of privacy. Criminal Tax Counsel and/or an Assistant United Stated Attorney review uses in excess of 30 days.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

The IP Camera System uses Video Management System (VMS) that controls user access and creates system logs of the activity of each user. System Administrators regularly monitor the system logs for any unusual activity including failed access attempts, excessive usage, and inactivity of user accounts.

27 Does this system use or plan to use SBU data in a non-production environment?

No

# Interfaces

**Interface Type**
    IRS Systems, file, or database
Agency Name
    IP Camera System
Incoming/Outgoing
    Incoming (Receiving)
Transfer Method
    Amazon Web Services Platform (AWS)

**Interface Type**
    IRS Systems, file, or database
Agency Name
    IP Camera System
Incoming/Outgoing
    Outgoing (Sending)
Transfer Method
    Secure File Transfer Protocol (SFTP)

# Systems of Records Notices (SORNs)

**SORN Number & Name**
    IRS 46.005 - Electronic Surveillance and Monitoring Records
Describe the IRS use and relevance of this SORN.
    IRS-CI is conducting electronic surveillance in support of the
    criminal investigations.

# Records Retention

What is the Record Schedule System?
    Record Control Schedule (RCS)
What is the retention series title?
    Criminal Investigation Records
What is the GRS/RCS Item Number?
    30 Part II Item 40
What type of Records is this for?
    Electronic
Please provide a brief description of the chosen GRS or RCS item.
    Investigative Files and Related Records

What is the disposition schedule?
> Destroy 10 years after case is closed.

# Data Locations

What type of site is this?
> System

What is the name of the System?
> IP Camera System

What is the sensitivity of the System?
> Sensitive But Unclassified (SBU)

Please provide a brief description of the System.
> Video Management System

What are the incoming connections to this System?
> IRS-CI managed Internet Protocol (IP) surveillance cameras are streamed into the Video Management System (VMS). All connections are limited to IRS-CI managed users with specific permissions. Access to the system is obtained through IRS-CI TaLON interface and through the mobile phone app on the IRS-CI manages devices.

What are the outgoing connections from this System?
> When required, a secure file transfer protocol is used to export a copy of a video files a part of the IRS-CI's legal obligation to provide discovery and is coordinated with the local United States Attorney's Office.