APPENDIX C

Template

Privacy Impact Assessment for the Use of CCTV

By

DHS Programs

Overview

The overview should include:

- The system or program's technical and commonly referred-to name and the Department of Homeland Security (DHS) Component and program responsible for its implementation and oversight.
- The name of the Federal, state, local, or other entities that operate, oversee, or have access to the system and program
- The objective of the program and how it relates to the mission of the program and DHS.
- A general description of the technology, the system, and the program.
    - Technology: for example, a description of the camera and recording technologies, with model numbers, vendors, and functions.
    - System: for example, a description of the network of surveillance devices—where and how they are installed, the number of devices, the system for collecting and, if applicable, monitoring the visual information.
    - Program: for example, a description of the law enforcement program that oversees or uses the surveillance technology – its development, funding, purpose, and limitations.

A clear and concise overview provides the reader the context in which to view the remainder of the PIA.

<< ADD Overview Here >>

Section 1.0 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed. The term "information" includes all images and footage captured by the camera system and any information associated with those images that can be linked to individuals. If the images are viewed but not stored, please indicate that process below.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's technology enables it to record:

☐ Video
    Static Range:
    Zoom Range:
    Pan from one angle to another:
☐ Tracking
    ☐ Automatic (for example, triggered by certain movements, indicators)
    ☐ Manual (controlled by a human operator)
☐ Sound
    Frequency Range:

Provide a description of what the camera is intended to view.
<<ADD Answer Here>>

The System typically records:

- ☐ Passersby on public streets.
- ☐ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
- ☐ Images not ordinarily available to a police officer on the street:
  - ☐ Inside commercial buildings, private homes, etc.
  - ☐ Above the ground floor of buildings, private homes, etc.

☐ The System does not record or store the images.

Sample screenshots of a typical recording may be a helpful item to include in an appendix to the PIA.

1.1.1 If the activity or program seeks any specific information or types of information, please specify what is being sought.

<< ADD Answer Here>>

1.1.2 Is the information obtained from the CCTV monitoring combined with any other information; and if so, please describe the other information.

<<ADD Answer Here>>

1.2 From whom is the information collected?

- ☐ General public in the monitored areas.
- ☐ Targeted populations, areas, or activities (please describe).
- ☐ Program personnel are directed to focus on particular people, activities, or places.

1.2.1 Describe any training, guidance, or policies given to program personnel that direct them to focus on particular people, activities, or places.

<< ADD Answer Here >>

1.3 Why is the information being collected? Identify all that apply.

- ☐ For traffic-control purposes
- ☐ Crime prevention
- ☐ Crime detection
- ☐ To aid in criminal prosecution
- ☐ Threat identification
- ☐ Terrorism investigation
- ☐ Terrorism prevention

☐ Other (please specify)

1.3.1 Policy Rationale

Provide a brief description stating why cameras are necessary to the program and to the governmental entity's mission. Description may address one or more of the following:

- ☐ Crime prevention rationale: (For example: (1) Crimes in-progress may only be prevented if the cameras are monitored in real-time. (2) A clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)
- ☐ Crime investigation rationale: (For example: A hidden camera may be investigative, providing after-the-fact records of persons and locations that may be subpoenaed.)
- ☐ Terrorism rationale: (For example: Video footage is collected to compare against information contained in terrorist databases.)

1.3.2 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features were selected to advance the program's mission. For example, describe how low-light technology was selected to combat illegal border crossing at night. It is not sufficient to merely state the general purpose of the system.

<< ADD Answer Here >>

1.3.3 Are you using the cameras to track and/or to identify individuals?

<<ADD Answer Here>>

1.4 How is the information collected?

- ☐ Real-time monitoring, with footage streamed, but not stored.
- ☐ Real-time monitoring with footage stored.
- ☐ Footage not monitored, only stored.

1.5 Operating Policies and Procedure

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

<< ADD Answer Here >>

1.6 Effectiveness

Describe how the program will evaluate the camera system's performance. Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

<< ADD Answer Here >>

1.7 Cost Comparison

Has the program done a cost comparison of the camera system to alternative means of addressing the system's purposes that may have less of an impact on privacy? If so, provide a summary of such cost comparison. (For example, compare the cost of the camera system to adding law enforcement personnel to patrol the area.)

<< ADD Answer Here >>

1.8 What specific legal authorities, arrangements, and/or agreements govern the camera system?

The section should include a description of the legislative authorization of DHS, as well as any executive or law enforcement decision authorizing the system. In addition, provide a list of the limitations or regulations controlling the use of the camera system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

<< ADD Answer Here >>

1.9 The Decision Making Process

Describe the decision making process that led to the purchase of the camera system.

- ☐ Decision-making process included public comment or review
- ☐ The Program making the decision relied on:
  - ☐ case studies
  - ☐ research
  - ☐ hearings
  - ☐ recommendations from camera vendors
  - ☐ information from other localities
  - ☐ other (please specify)

<< ADD Answer Here >>

1.10 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use, discuss what privacy risks were identified and how they were mitigated. If during the system design or technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks you can discuss include:

- **Privacy rights**. For example, cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, or an Alcoholics Anonymous, social, political, or religious meeting.
- **Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or associations between individuals. Such recording may chill constitutionally-protected expression and association.

- **Government accountability and procedural safeguards**. While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, including creating a system of accountability for all uses.
- **Equal protection and discrimination**. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, such as profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation, or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.

  << ADD Answer Here >>

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the footage or images derived from the cameras.

Please describe in detail how the footage or images are used, as well as how the footage or images may be used in the future.

<< ADD Answer Here >>

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that the footage or images is handled in accordance with the above described uses. For example, is appropriate use of the information covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the technology or records?

<< ADD Answer Here >>

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the information in the system (i.e., how long are footage or images stored)?

- ☐ 24-72 hours
- ☐ 72 hours – 1 week
- ☐ 1 week – 1 month
- ☐ 1 month – 3 months
- ☐ 3 months – 6 months
- ☐ 6 months – 1 year
- ☐ more than 1 year (please describe)

☐ indefinitely

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

<< ADD Answer Here >>

3.2 Retention Procedure

☐ Footage or images are automatically deleted after the retention period expires
☐ System operator required to initiate deletion
☐ Under certain circumstances, officials may override detention period:
  ☐ To delete the footage or images before the detention period
  ☐ To retain the footage or images after the detention period
  ☐ Please describe the circumstances and official process for override

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the designated period.

<< ADD Answer Here >>

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the program's operation, for example, sharing with various units or divisions within the Component or DHS. *External sharing with outside entities will be addressed in the next section.*

4.1 With what internal entities and types of personnel will the information be shared?

Internal Entities
☐ Investigations unit
☐ Auditing unit
☐ Financial unit
☐ DHS enforcement unit
☐ Other (please specify)
☐ None

Types of Personnel
☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☐ Other (please specify)

4.2 For the internal entities listed above, what is the extent of the access each receives (i.e. what records or technology is available to them, and for what purpose)?

<< ADD Answer Here >>

4.2.1 Is there a written policy governing how access is granted?

- ☐ Yes (please detail)
- ☐ No

4.2.2 Is the grant of access specifically authorized by:

- ☐ Statute (please specify which statute)
- ☐ Regulation (please specify which regulation)
- ☐ Other (please describe)
- ☐ None

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

- ☐ Off-site, from a remote server
- ☐ Via copies of the video distributed to those who need it
- ☐ Only by viewing the video on-site
- ☐ Other (please specify)

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

<< ADD Answer Here >>

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including other Federal agencies, State and Local Government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or images and related information will be shared. The term "external entities" refers to individuals or groups outside your organization.

- ☐ Local government agencies (please specify)
- ☐ State government agencies (please specify)
- ☐ Federal government agencies (please specify)

- ☐ Private entities:
  - ☐ Businesses in monitored areas
  - ☐ Insurance companies
  - ☐ News outlets
  - ☐ Other (please specify)
- ☐ Individuals:
  - ☐ Crime victims
  - ☐ Criminal defendants
  - ☐ Civil litigants
  - ☐ General public via Public Records Act or Freedom of Information Act requests
  - ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe all of the following:

- ☐ The purpose for disclosure
- ☐ The rules and regulations governing disclosure
- ☐ Conditions under which information will not be disclosed
- ☐ Citations to any specific authority authorizing sharing of the camera footage or images

5.3 How is the information transmitted or disclosed to external entities?

- ☐ Discrete portions of camera footage or images are shared on a case-by-case basis
- ☐ Certain external entities have direct access to camera footage or images
- ☐ Real-time feeds of footage or images between agencies or departments
- ☐ Footage or images are transmitted wirelessly or downloaded from a server
- ☐ Footage or images are transmitted via hard copy
- ☐ Footage or images may only be accessed on-site

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with each external organization with whom information is shared, and does the MOU reflect the scope of the information currently shared?

- ☐ Yes
- ☐ No

If an MOU is not in place, explain steps taken to address this omission.

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)
☐ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☐ Technological protections do not remain intact once information is shared

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your program/component?

<< ADD Answer Here >>

Section 6. 0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Program leadership
☐ Operation personnel
☐ Persons outside the program who will have routine or ongoing access to the system (please specify)
☐ Other (please specify)

6.1.1 Are different levels of access granted according to the position of the user? If so, please describe.

☐ All authorized users have access to real-time footage or images
☐ Only certain authorized users have access to real-time footage or images (please specify which users)
☐ All authorized users have access to stored footage or images
☐ Only certain users have access to stored footage or images (please specify which users)
☐ All authorized users can control the camera functions (pan, tilt, zoom)
☐ Only certain authorized users can control the camera functions
☐ All authorized users can delete or modify footage or images

☐ Only certain authorized users can delete or modify footage or images (please specify which users)

6.1.2 Are there written procedures for granting access to users for the first time?

☐ Yes (please specify)
☐ No

6.1.3 When access is granted:

☐ There are ways to limit access to the relevant records or technology (please specify)
☐ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

☐ To monitor who accesses the records?
☐ To track their uses?

6.1.5 Training received by prospective users includes discussion of:

☐ Liability issues
☐ Privacy issues
☐ Technical aspects of the system
☐ Limits on system uses
☐ Disciplinary procedures
☐ Other (specify)
☐ No training

The training lasts:

☐ None
☐ 0-1 hours
☐ 1-5 hours
☐ 5-10 hours
☐ 10-40 hours
☐ 40-80 hours
☐ More than 80 hours

The training consists of:

☐ A course
☐ A video
☐ Written materials
☐ Written materials, but no verbal instruction
☐ None
☐ Other (please specify)

6.2 The system is audited:

- ☐ When an employee with access leaves the organization
- ☐ If an employee is disciplined for improper use of the system
- ☐ Once a week
- ☐ Once a month
- ☐ Once a year
- ☐ Never
- ☐ When called for

6.2.1 System auditing is:

- ☐ Performed by someone within the organization
- ☐ Performed by someone outside the organization
- ☐ Overseen by an outside body (for example a city council or other elected body – please specify)

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

<< ADD Answer Here >>

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of camera recording that they are within view of a camera?

- ☐ Signs posted in public areas inform the public of recording by cameras
- ☐ Signs in multiple languages
- ☐ Attached is a copy of the wording of such notice signs
- ☐ Notice is not provided
- ☐ Other (please describe)

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the camera system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

- ☐ Yes
- ☐ No

8.2 What design choices were made to enhance privacy?

- ☐ The system includes face-blurring technology
- ☐ The system includes blocking technology

☐ The system limited location to address privacy
☐ The system has other privacy-enhancing technology (Please specify)
☐ None (Please specify)

Section 9.0 – Attachments to the PIA

☐ Authorizing legislation
☐ Grant documents
☐ Transcript of public hearing or legislative session
☐ Press release announcing the CCTV program
☐ Program manuals outlining the system's rules and regulations
☐ Other (please specify)

Responsible Officials

<< ADD Privacy Officer/Project Manager>>

Approval Signature

_____

Chief Privacy Officer
Department of Homeland Security