**APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT**

| | |
|---|---|
| **Department or Division:** | Somerville Police Department (SPD) |
| **Compliance Officer (name and position):** | Lt. Jeff DiGregorio |
| **Submitted by:** | Lt. Jeff DiGregorio |
| **Date:** | |
| **Surveillance Technology:** | Covert Device Cameras |

| *X* | **Please identify the purpose(s) of the proposed surveillance technology. Select ALL that apply by entering "X" in the left column.** |
|---|---|
| x | Identifying and preventing threats to persons and property and preventing injury to persons or significant damage to property |
| x | Identifying, apprehending, and prosecuting criminal offenders |
| x | Gathering evidence of violations of any law in criminal, civil, and administrative proceedings |
| x | Providing information to emergency personnel |
| | Documenting and improving performance of City employees |
| | Executing financial transactions between the City and any individual engaged in a financial transaction with the City |
| | Preventing waste, fraud, and abuse of City resources |
| | Maintaining the safety and security of City employees, students, customers, and City-owned or controlled buildings and property |
| | Enforcing obligations to the City |
| | Operating vehicles for City business |
| | Analyzing and managing service delivery |
| | Communicating among City employees, with citizens, or with third parties |
| | Surveying and gathering feedback from constituents |
| | Other (Describe):<br><br>If the surveillance technology is used for a purpose not listed above, does the purpose comply with the surveillance use policy? _x__ Yes ___ No |

**Complete ALL of the following items related to the proposed surveillance technology. Be as specific as possible. If an item is not applicable, enter "N/A." Do NOT leave fields blank.**

1. Information describing the surveillance technology and how it works:

3 covert cameras are hidden in household devices (alarm clock, smoke detector and computer speaker). During the course of a criminal investigation these cameras would be placed in the suspect's home/business under authority of a search warrant. These cameras have been used in public areas as well. For example, cameras have been previously placed in common areas in private buildings, where there is no expectation of privacy; public areas, such as city streets and open spaces; and city owned buildings. Under current case law, a search warrant would be required to use this device if it captured entrances to homes and other places where there would be an expectation of privacy. These devices are kept in two locations.

1, The Family Services Sergeant's office, under his/her direct control.

2, The Narcotics/Vice Sergeant's office, under his/her direct control.

The SPD will determine the requirements of obtaining a search warrant prior to the installation of a covert camera based on the most current procedural law established through the Massachusetts Court. The current case being Comm v. Mora.

a. Authorized use – the uses that are authorized, the rules and processes required before that use, and the uses that are prohibited (10.64.b.2):

The SPD will implement the following procedure, "The use of any covert device will require the establishment of an open investigation and the assignment of an incident number for tracking purposes. The Captain of CID (Criminal Investigations Division) will be presented with the facts requiring the use of such device and will be responsible for its authorization. The Captain of CID will notify the Family Services Sergeant or the Narcotics/Vice Sergeant, authorizing the use of such devices. The sergeant will maintain a sign-out sheet, containing the Detectives name, date of sign out, incident number and date of return. The sergeant will be responsible for overseeing the investigation. Placement of the camera would follow the aforementioned requirements and be in compliance with all applicable state laws and department policy."

b. Training – the training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials (10.64.b.9):

There would be a very limited number of investigators using this tool. These devices are secured by a detective supervisor and would only be used at their direction. No formal training would be required as it is a simple device controlled manually or remotely with video stored on a department computer only accessible by that individual detective.

Detectives receive both classroom and field training at the start of their assignments in CID. This training comes from both internal and external sources (Advanced Criminal Investigation & Crime Scene training). This procedure will be overseen by one of the two aforementioned Sergeants. The Appeals Division of the Middlesex District Attorney's Office is available 24/7 regarding matters of concern.

2. Information on the proposed purpose(s) for the surveillance technology (10.64.b.1):

This technology would be used in criminal investigations. This would be available in civil proceedings, in response to the necessary court process and after consultation with the Somerville Law Department.

3. Information describing the kind of surveillance the surveillance technology is going to conduct and what surveillance data is going to be gathered (10.64.b.3):

This technology would be used in criminal investigations and would gather video evidence in the course of the investigation.

a. Data access – the individuals who can access or use the collected surveillance data, and the rules and processes required before access or use of the information (10.64.b.4):

The device would be used at the direction of the Captain overseeing CID, and would be used in accordance with Massachusetts law, the section of the City's Surveillance Technology Use Policy entitled "Video Surveillance Technology, Data and Use by the Police Department", and department policy.

b. Data protection – the safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms; (10.64.b.5)

The video would only be accessible to the investigator and the supervisor, requiring a login and password. Storage would be made on a department computer which is only accessible by the investigator. Dissemination of any footage will require authorization from one of the aforementioned sergeants.

c. Data retention – the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period has elapsed, and the conditions that must be met to retain information beyond that period (10.64.b.6):

The images and video would be retained for the duration of the criminal investigation and if applicable any court proceeding. Information retrieved from the covert devices that poses a direct threat to Office safety would be distributed throughout the department and regional partners by an "Officer Safety" bulletin from our Crime Analysts. The Family Services and/or Narcotics/Vice Sergeant(s) will be responsible for authorizing the release of such material.

d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):

The video and images are subject to criminal and civil procedure discovery rules. Any public information request would be vetted through the City's Law Department.

e. Third-party data-sharing – if and how other city or non-city entities can access or use the surveillance data, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the surveillance data (10.64.b.8):

Evidence could be shared depending on the investigation and if other law enforcement agencies are involved or affected or if there is a public safety threat. Images/video would be shared with the District Attorney's office as part of submitting evidence for a criminal case. Images could be shared if there was a joint investigation with another Law Enforcement agency such as the State Police or the FBI. Images would only be shared with members of the investigating group who had permission to use these devices.

In the event that a direct threat to officer safety is observed from the covert device, the aforementioned sergeant(s) would authorize the dissemination of this particular threat to our regional partners through our Crime Analyst(s).

4. The location(s) it may be deployed and when:

This would be case specific and depend on the type of investigation. Placement and use of the cameras would be regulated under Massachusetts law, the section of the City's Surveillance Technology Use Policy entitled "Video Surveillance Technology, Data and Use by the Police Department", and department policy.

5. A description of the privacy and anonymity rights affected and a mitigation plan describing how the department's use of the equipment will be regulated to protect privacy, anonymity, and limit the risk of potential abuse:

The cameras are only accessible by a supervisor in the detective bureau and could not be used without that individual supervisor's knowledge. The camera would only be used with permission of a supervisor and used under authorization of a search warrant or other applicable Massachusetts laws. It would also be used in accordance with the section of the City's Surveillance Technology Use Policy entitled "Video Surveillance Technology, Data and Use by the Police Department".

6. The potential impact(s) on privacy in the city; the potential impact on the civil rights and liberties of any individuals, communities or groups, including, but not limited to, communities of color or other marginalized communities in the city, and a description of whether there is a plan to address the impact(s):

This technology is used during a criminal investigation under guidelines and laws laid out by the state and department. It is used to surveil a particular suspect and would not be used outside the particular house or business that is subject to that particular investigation. This device could be used in a common area or other place where there is no expectation of privacy with the sound recording disabled if it met the requirements under Massachusetts Procedural Law but in most cases would be used under the authority of a search warrant. These devices are not arbitrarily placed and would not surveil anyone outside the scope of the investigation and those that are authorized to be viewed. (See Comm V. Mora)

7. An estimate of the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding:

The devices cost approximately $300 and there are no ongoing costs associated with covert cameras.

8. An explanation of how the surveillance use policy will apply to this surveillance technology and, if it is not applicable, a technology-specific surveillance use policy:

This technology involves filming and obtaining images of individuals during the course of a criminal investigation. Based on this, the city's surveillance policy would apply to this particular technology.

a. Oversight – the mechanisms to ensure that the surveillance use policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the surveillance technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy (10.64.b.10):

One of the aforementioned Detective Sergeants would oversee the use of this camera and be responsible for the camera's storage and distribution (after receiving authorization from the Captain of CID). Other detectives who could view and pull footage would have to have the authorization from a detective supervisor. Violations of this policy and misuse of camera technology would lead to departmental discipline up to and including termination.