

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:	Homeland Security 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
	Identifying, apprehending, and prosecuting criminal offenders
	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): If the surveillance technology is used for a purpose not listed above, does the purpose comply with the surveillance use policy? ___ 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:

Technology is owned and operated by the Federal Government. These cameras are used to monitor evacuation routes around Boston and adjacent towns. Somerville police have access to the video feed and video can be preserved.

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):

These cameras can be accessed by the police department in cases of public emergency or to investigate a crime. The camera's primary use is to monitor traffic routes. The Homeland Security sergeant is the primary liaison for the company that maintains them, Lantel, and the Federal Government. Cameras can be accessed in case of public emergency, accident investigation, or criminal investigation.

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):

Lantel, the company that installs and maintains the cameras, offers training in their use.

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

The purpose of these cameras is to monitor major evacuation routes around the Boston metro area.

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):

The cameras are not intended for surveillance. As stated, their main function is to monitor routes in the Boston area and surrounding towns in the case of an emergency requiring an evacuation. The cameras do however record public roads in the City of Somerville and this footage has been used in the investigations for both crimes and for serious motor vehicle accidents.

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 traffic department, detectives, patrol supervisors, station officers, IT, and crime analysis can access these cameras. The cameras run on a live loop throughout the city.

<p>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)</p>
<p>There is a login for access to camera views and data preservation. Only authorized users would have login credentials. The login record is preserved through the IT department and would be able to be viewed in the instance of suspected misuse.</p>
<p>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):</p>
<p>Video is kept on the server for approximately 30 days and then overwritten unless preserved for a longer period for the purpose of an investigation.</p>
<p>d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):</p>
<p>Public information requests can be made and based on approval from the city’s law department can be granted. Footage may be subject to discovery in criminal cases and subpoenas in civil cases.</p>
<p>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):</p>
<p>Footage can be shared with other law enforcement agencies per their request in regards to criminal or motor vehicle accident investigations or initiated by SPD as part of an SPD active investigation.</p>
<p>4. The location(s) it may be deployed and when:</p>
<p>Approximately 30 working cameras are dispersed across the city on public roads and intersections at fixed conspicuous locations. Cameras can be moved, only with approval from FEMA, if there is a stated safety need by the city or for legitimate law enforcement necessity. Current list and location is available upon request.</p>
<p>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:</p>
<p>Cameras are located on public roadways where there would be no expectation of privacy. They do not record</p>

sound. Locations of cameras are recorded and cameras cannot be moved to record private property or residences. Anyone accessing and using a recording would be documented through IT.

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):

Cameras are installed by Homeland Security in locations based on emergency evacuation route planning. These routes connect to those in Boston and other surrounding cities.

Log in procedures and recording authorization would track users and ensure all use and recordings would be for approved criminal investigation or traffic investigation. Any movement of fixed cameras would need to be reported to the federal government and could be moved for only a legitimate law enforcement or emergency reason.

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:

UASI funds paid for installation and maintenance of the cameras so there is no cost to the city.

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:

Since this technology records visually the city's policy would apply.

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):

The Homeland Security Sergeant would oversee the use of these cameras. Supervisors, Detectives, and Crime Analysis can view and download footage. This access is dependent on authorization from the individuals' immediate supervisor.

The system generates an access log, which can be preserved if necessary through the IT department, that tracks username log-ins. This would allow for monitoring and identification of who used the technology and when. Violations of this policy and misuse of camera technology can lead to oral reprimand, written reprimand, suspension, or termination depending on the actions.