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:	License Plate Readers

X	**Please identify the purpose(s) of the proposed surveillance technology. Select ALL that apply by entering "X" in the left column.**
	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): 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:

(SPD does not currently use this technology but has in the past and may in the future)

Readers installed on top of police vehicles automatically scan license plates and run information through the RMV. Officers are alerted for license, registration, or WMS infraction. The technology eliminates the need to manually input license information and does not grant any extra access that is not already available from the RMV.

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):

All officers using this technology would have to have login credentials and all their activity would be tracked. RMV information could only be accessed for official law enforcement purposes only.

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):

The technology is relatively simple and user friendly. The system alerts the officer of a "hit". A "hit" such as a warrant, expired registration, licences, etc. would have to be confirmed manually through the RMV database. Once the readers are activated there is nothing for the officer to do but confirm a violation through the RMV database.

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

This technology only streamlines tools already available to officers and 911 personnel. It would eliminate the need for officers to manually enter data while operating a police vehicle and makes enforcement activities safer and more efficient.

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 technology would gather RMV information such as registration, license status, driver's history, and driver information. This RMV information is already accessible through Mobile Data Terminals in police vehicles.

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):
All sworn personnel would be authorized to use this technology. Officers would be required to log into the technology and activate it. All information would have to be confirmed manually through the RMV
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)
This technology would only be in a police vehicle and results would be returned on MDT in vehicle. The officer logged into the program would be the only person able to view the information
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):
Data retention would be determined by the RMV and at the time of use in the future. As of last known retention time it was approximately 60 days
d. Public access – if and how collected surveillance data can be accessed by members of the public, including criminal defendants (10.64.b.7):
This technology only streamlines existing technology, eliminating the need to manually enter licence plate information. Rules regarding public access to this information would be regulated by the RMV, Massachusetts law, and department policy.
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):
This technology only accesses RMV information and it would be shared depending on criminal or civil motor vehicle investigations
4. The location(s) it may be deployed and when:
LPR would be installed on police vehicles which operate continuously once the application is opened.

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:

There is no expectation of privacy for information obtained via a registration check. All information that is picked up by the LPR is already accessible by officers using their MDT. This technology only makes access more efficient.

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 picks up information about cars that pass by it. These devices would be used on public roadways within the city. This technology operates constantly as it is attached to police vehicles and scans cars on city roads as officers pass by them.

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:

Unknown at this time as it would depend on how many vehicles would be outfitted and the cost of equipment at the time of installation.

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 the device captures images the city surveillance 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):

This technology would have a log on function and all officers would be tracked when they accessed the LPR. There is an access log available to view who has logged onto the system and see what plates were individually queried. This would allow for monitoring of who is using this technology. Besides supervisors at the police department, the RMV monitors license plate and driver information being queried. They can be sanctioned for misuse up to suspending the department's operating license through RMV. Violations of this policy and misuse of LPR technology can lead to department discipline up to and including termination.