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:	GreyKey

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
	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:

The Somerville Police Department does not possess this technology, but have used it in the past with the cooperation of the Massachusetts Attorney General's Office and plan to continually use this technology. This technology opens locked devices (computers and cell phones) by bypassing any passcodes to gain access to the device.

The Detective would go to the AG's Office with the device. Under the guidelines of the AG's Office and the laws of the Commonwealth, the devices would be accessed (Search Warrant or Consent).

The AG's Office currently uses the Premium version of the GreyKey software, but the versions of the software are subject to updates; provided, that the core function of the technology remains consistent with the description and use herein.

The Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA) and State Police also have access to this technology. While Somerville Police Department generally goes through the AG's office to use this technology, there may be instances where the Department would access the technology through one of these other agencies.

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):

This device would be used only under the authorization of a search warrant, and such use would be subject to relevant case law. Similar to searches of a person's car or home, searches of someone's phone are subject to limitations laid out in case law, and the scope and terms of the warrant. There is a high bar for getting a warrant to infiltrate someone's phone, and while the area of law is still evolving as technology evolves, the court has been strict about the scope of information that can be gathered from a phone search.

The technology cannot be used to collect personal information unrelated to the investigation; the information gathered must be relevant to the investigation as indicated in the search warrant.

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):

One detective is trained in using this device and is currently the only member of the department qualified to operate this technology. This individual is assigned to General Detectives/Digital Forensics. This Detective has attended multiple training classes, on numerous platforms and must do so yearly inorder to maintain certification.

In addition, the Detective authorized to use this technology would receive the training required pursuant to the Surveillance Technology Use Policy.

If any additional detectives are authorized to use this technology in the future, they would need to do so in accordance with this impact report and would receive training as required by the Surveillance Technology Use Policy.

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

This device would only be used in cases in which a search warrant has been obtained in conjunction with the investigation allowing access to the device in question or with the owner's consent.

One example for the use of this technology would be to gain access to a suspect's phone, in order to obtain his location at a specific date and time. ie...An innocent victim was shot.

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 opens "locked" devices by overriding passcodes and thus accessing the content on the device.

Surveillance information obtained covers a wide spectrum of crimes, the majority of the time are violent in nature. Computers and phones have been accessed to convict for Child Pornography, Murder/Attempted Murder, Armed Robbery and Shots Fired incidents, just to name a few examples.

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):

Only the investigator and investigator's supervisor would have access to the data recovered.

Information retrieved is stored on one specific computer, under the direct control of the Digital Forensics Detective. This information is distributed to the investigating Detective and the District Attorney's Office only.

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 device is used by one member of the detective bureau and under the direction of a supervisor and under the authorization of a search warrant. The information and data accessed is stored remotely and password protected, and is not stored on the SPD's general server. In addition, the data accessed is subject to confidentiality.

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):

This would not apply as the device unlocks computers and phones and does not collect data. However, any evidence obtained from using this device would be retained for the duration of the investigation and pending legal processes.

The length of retention time varies, based on various factors, such as: length of the investigation and the statute of limitations set by the Commonwealth.

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

There would be no data collected but access to electronic devices. Thus there would be no public access to information obtained per se. The information obtained via seizing the device would be subject to discovery rules. Criminal defendants could request information through discovery rules.

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 would be used specifically to named investigations and under the authority of a search warrant. There would be no third party sharing (besides turning evidence over to the District Attorney's Office for prosecution) unless the investigation involved another law enforcement agency or if the crimes investigated were multi-jurisdictional.

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

This device would only be deployed in investigations under authority of supervisor's approval and search warrant.

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 device would be used by a single trained member of the department, under the authorization of a supervisor, and only with consent or a search warrant.

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 device would be used specifically, in conjunction with an active criminal investigation. Any authority to use this device would be granted by a search warrant, and could not be used indiscriminately.

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:

There is no cost as this device is not owned by the city nor the police department, however there may be costs associated with training any new authorized users in the future.

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 device can look at data in locked devices 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):
There is only one investigator trained and authorized to use this device. Its use is first authorized by a detective supervisor, and also by the laws of the Commonwealth and under authority of a search warrant. Any misuse of this device would lead to department discipline up to and including termination.