APPENDIX A: SURVEILLANCE TECHNOLOGY IMPACT REPORT

Department or Division:	Somerville Police Department (SPD)
Compliance Officer (name and position):	Lieutenant Kevin Shackelford
Submitted by:	Lieutenant Kevin Shackelford
Date:	May 11, 2026
Surveillance Technology:	CrimeTracer

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
X	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
X	Analyzing and managing service delivery
	Communicating among City employees, with citizens, or with third parties
	Surveying and gathering feedback from constituents
X	Other (Describe): Crime Tracer Database used for POST certification 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:

CrimeTracer is a police collaborative software system that links criminal justice data from multiple agencies. Police report data is pushed out from Somerville Police Department's records management system to CrimeTracer's database once a day through an automated IT process.

According to SoundThinking Inc. (the makers of CrimeTracer), Artificial Intelligence (AI) has been integrated into the CrimeTracer application. CrimeTracer includes optional AI-assisted features designed to support investigative efficiency, such as: Search using natural-language with AI Chatbot, AI-generated summaries of records and documents, and AI assistance for identifying relevant patterns or relationships already present in agency data. These AI features augment analyst workflows but do not replace investigative judgment.

CrimeTracer AI accesses data already available within the agency's CrimeTracer environment and records and entities that users are authorized to view. AI cannot access external systems, hidden databases, or information outside of configured integrations. AI interactions are stored for auditing and CJIS compliance purposes. AI interaction data is not shared across agencies. AI features (Chatbot, Summarization, Entity Extraction) in CrimeTracer are optional and controllable by administrators. Agencies may disable all AI features at any time or enable only specific AI capabilities.

AI does not bypass or weaken existing security controls. CrimeTracer positions AI as a time-saving aid, not a source of truth. Original records and linked data remain the authoritative source. CrimeTracer AI features help users navigate, summarize, and explore existing information more efficiently

CrimeTracer does NOT use AI:

- To perform surveillance or real-time monitoring
- For facial recognition, biometric identification, or person-tracking (AI features do not identify individuals based on images, video, or biometric attributes.)
- To generate enforcement decisions
- To train, retrain, or improve AI models using agency data
- To Modify, overwrite, or alter source records. All AI outputs (such as summaries) are derived views, clearly identified with AI-specific coloring.

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):

Authorized users are only those who are verified public safety personnel. Access is strictly controlled by the user's agency and the Commonwealth Fusion Center. The system is for official public safety purposes only and other use of the system is strictly prohibited. The system maintains logs on who and when data has been accessed.

The Commonwealth Fusion Center maintains records of users with access to the system and prohibits Federal Law Enforcement agencies as well as the military from accessing the CrimeTracer system.

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):

No training is required. Users are strongly encouraged to attend training provided by the Commonwealth Fusion Center.

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

This technology allows the SPD to obtain nationwide crime data (from participating agencies) on a daily basis to help effectively solve crime and address crime issues in the community. Additionally, a query of "Coplink" (now CrimeTracer) is required for Police Officer certification according to the Peace Officer Standards and Training Commission's "Agency Intake Form".

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):

Data contained in CrimeTracer includes arrest reports, incident reports, citations, booking photos and information, vehicle information, probation/parole records, warrants (court information), field interviews and observations, and administrative messages.

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):

Data access is controlled by the user's agency and the MSP Fusion Center. Data is for official use only. Use of this technology falls under the City's Surveillance Technology Use Policy. Additionally, users receive advisements about system access requirements and prohibitions each time they log into the system. These advisements state:

- You are accessing a restricted information system.
- Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
- Use of the system indicates understanding of the above and consent to monitoring, recording and audit.
- **WARNING!** The use of publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access this information system is unauthorized. This type of usage may result in the involuntary dissemination of information to unauthorized entities. Data may be left on this computer resulting in the next person using this machine the ability to view your data.

Users in Massachusetts may access records from agencies outside the state. However, records originating in Massachusetts are only accessible to users within the state.

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)

Data protection falls under the City's Surveillance Technology Use Policy and the CrimeTracer user agreement (noted in 3a). According to Soundthinking Inc. (vendor of CrimeTracer), the application is encrypted and meets CJIS requirements via FIPS 140-2/3 standards. All data is secured using AES-256 (FIPS 197 compliant) at rest and TLS 1.2+ in transit. Additionally, there is a layered process for gaining access to the system, in that it can only be accessed on networks authorized by the Commonwealth Fusion Center, by users granted access by the Commonwealth Fusion Center, who must use an authenticator application (linked to the user) to log in.

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):

Information provided to CrimeTracer is retained for an indefinite period of time. Records will remain in CrimeTracer as long as they exist within a participating law enforcement agency's records management system. (Note: If records were removed from a participating Law Enforcement Agency's records management system, they would also be removed from CrimeTracer.)

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

Members of the public can make a Public Records Request in writing through the Department's Records Clerk or

the City's Records Access Officer. This request is then forwarded to and/or reviewed by the City of Somerville Law Department, who will issue a response subject to applicable exemptions, if any, under the Public Records Law. Though police reports and data from other agencies may be available in CrimeTracer, requestors must request this information from the originating police department not the Somerville Police Department. (Note: there are exceptions which include records from CrimeTracer that have been saved, printed, attached to a report, or referenced in a case file by SPD personnel as these would be subject to public records requests.)

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):

Information 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. When submitting CrimeTracer records as evidence for a criminal case, the data would be shared with the District Attorney's office in accordance with Massachusetts Rules of Evidence. Information may also be shared with Human Resources as part of background investigations during the police hiring process and with the Peace Officer Standards and Training (POST) Commission as part of the certification process.

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

CrimeTracer is a web-based database application that is available on the department's network or computers using an approved IP address.

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 CrimeTracer system is operated under the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations [CFR] Part 23). All member agencies have agreed to comply with the requirements of 28 CFR Part 23 with respect to any criminal information they submit into applicable CrimeTracer databases.

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):

The Somerville Police has a Biased Based Policing Policy (#115). This policy emphasizes the Department's commitment to protecting the Constitutional and civil rights of all members of the community. Officers are trained annually on this policy. The SPD expresses its commitment to preserving and respecting the Constitutional rights of all the members of the community. The SPD does not endorse, train, teach, support, or condone any type of bias, stereotyping, or racial and gender profiling by its employees.

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:

CrimeTracer is funded by the Executive Office of Public Safety and Security (EOPSS) in Massachusetts. 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:

The City's Surveillance Technology Use Policy applies due to the fact that the application is used for data collection. "Data Collection" is specifically cited in the City of Somerville's Surveillance Technology Use policy. This application compiles law enforcement data.

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):
Oversight is conducted at the Department level through the Chain of Command. The Commonwealth Fusion center may utilize audit functions internal to the system if a report of misuse is received. The Surveillance Technology Use Policy, all SPD policies and all applicable Massachusetts laws apply. Misuse of CrimeTracer will be addressed by the Chief or Police and/or the SPD Office of Professional Standards on a case-by-case basis depending on the circumstances. Violation of this policy and misuse of this technology could lead to departmental discipline up to and including termination.