Sec. 18-12-193. Surveillance Technology Specification Reports.

(a) The contents of the Surveillance Technology Report shall reflect the complete and accurate proposed use of surveillance technology being submitted.

(b) The Surveillance Technology Report shall be a publicly released report, written by the requesting agency or, in the case of the Police Department, in conjunction with the Board of Police Commissioners, that includes, at a minimum, the following:

1. *Description*: Information describing the surveillance technology and its capabilities;

DPD Response: The planned 31.8 square mile infrastructure expansion (which will bring the total coverage to 38.3 square miles) will utilize gunshot detection system sensors for incident monitoring and public safety purposes. The detection equipment will also allow for a detailed forensic report including detailed information of the gunshot detection incident, including: the number of rounds fired, the number of shooters involved, and the direction and speed of a shooter-in-motion.

2. *Purpose*: What specific purpose(s) the surveillance technology is intended to advance.

DPD Response: The purpose of this technology is to detect outdoor audible gunfire within the coverage area using acoustic sensors capable of pinpointing the accurate location of a gunfire event. This technology is used to address crime in real-time and support criminal investigations.

3. *Deployment*: If the surveillance technology will not be uniformly deployed or targeted throughout the City, what factors will be used to determine where the technology is deployed or targeted;

DPD Response: DPD identified the deployment based on crime data and logistics considerations.

4. *Fiscal Impact*: The fiscal impact of the surveillance technology; and

DPD Response: The expenditure for the expansion of service will be paid by General Funds. The contract's total cost is $7,000,000.00.

5. *Civil Rights/Liberties Impacts*: An assessment identifying with specificity:
    a. Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and
    b. What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts identified in this section.

DPD Response: Within already codified portions of the DPD Manual, DPD makes clear that members may not violate anyone's rights (Bias-Based Policing Policy 102.2). Additionally, civil liberty protections are outlined in this specific policy (Gunshot Detection System 307.8). Specifically, these provisions are:

307.8 - 3 Civil Liberty Protections

307.8 - 3.1 Strict Limitations on Access to Audio from Acoustic Sensors

1. Members shall only have access to recorded audio from confirmed gunshot incidents.

2. Members shall not be able to monitor live audio from acoustic sensors.

3. The recorded audio shall only be reviewable when pertinent to an active investigation involving a firearm discharge.

4. Any violations of this section of the directive shall be deemed egregious conduct and members shall be subject to discipline up to and including termination.

307.8 - 3.2 Private Residence and Buildings

A ShotSpotter alert, by itself, does not give responding Department member(s) the legal authority to enter private residence, private buildings, and the constitutional curtilage surrounding those properties.

307.8 - 3.3 ShotSpotter as Investigative Lead

Members shall not arrest solely on a ShotSpotter notification. As it is a lead only, any possible connection or involvement of any subject to the ShotSpotter notification must be determined through further investigation and investigative resources. An arrest must be based upon the totality of circumstances gathered from a thorough investigation.

6. *Authorized Use*: For what specific capabilities and uses of the surveillance technology is authorization being sought, and
    a. What legal and procedural rules will govern each authorized use;
    b. What potential uses of the surveillance technology will be expressly prohibited;
    c. Who, by employment category or position, will be authorized to operate the technology and/or access its data; and
    d. How and under what circumstances will surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology be analyzed and reviewed.

DPD Response: DPD has a Data Sharing Policy (101.12) that sets forth the standard the Department must follow when sharing data. DPD will also comply with any constitutional applicable law and Criminal Justice Information System (CJIS) policies. DPD will also provide the Gunshot Detection System policy (307.8) as a supplement.

7. *Data Collection*:
    a. What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;
    b. What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and
    c. How inadvertently collected surveillance data will be expeditiously identified and deleted.

DPD Response: Gunshot Detection Systems provide data on the location of a gunfire event, the number of rounds detected, and the direction and speed of a shooter. When a gunshot like sound triggers the sensor, the audio data is sent to ShotSpotter's Incident Review center for verification. Once qualified as a firearms discharge, the event is pushed to the ShotSpotter Respond application (on browser and mobile devices) and the ShotSpotter Dispatch application for member dispatch and investigation. DPD is only provide with audio beginning one (1) second prior to the gunshot and ending one (1) second after the final gunshot of the detected event.

8. *Data Protection*: what safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.

DPD Response: The Detroit Police Department will comply State of Michigan Criminal Justice Information System (CJIS) regulations and other applicable standards and policy to protect data. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related Department activity.

9. *Data Retention*: insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, what rules and procedures will govern the retention of surveillance data, including those governing:
    a. The limited time period, if any, surveillance data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Technology Specification Report;
    b. The specific conditions that must be met to retain surveillance data beyond the retention period identified pursuant to Subsection (9)(a) of this section;
    c. The process utilized to regularly delete surveillance data after the retention period stated in Subsection (9)(a) of this section has elapsed and the auditing procedures that will be implemented to ensure data is not improperly retained;

DPD Response: DPD has an existing Data Retention Policy (101.11) that matches the requirements set forth by the State.

10. *Surveillance Data Sharing*: if a municipal agency is seeking authorization to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities in the absence of a judicial warrant or other legal mandate, it shall detail:

a. Which governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities will be approved for (i) surveillance technology sharing, and for (i) surveillance data sharing;
b. How such sharing is necessary for the stated purpose and use of the surveillance technology;
c. How it will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable Surveillance Technology Specification Report and does not further disclose the surveillance data to unauthorized persons and entities; and
d. What processes will be used to seek city council approval of future surveillance technology or surveillance data sharing agreements

DPD Response: DPD has a Data Sharing Policy (101.12) that sets forth the standard the Department must follow when sharing data. DPD will utilize the Gunshot Detection System policy (307.8) as an additional guide.

11. *Demands for access to surveillance data*: what legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.

DPD Response: DPD has a Data Sharing Policy (101.12) that sets forth the standard the Department must follow when sharing data. DPD will also comply any constitutional applicable law and Criminal Justice Information System (CJIS) policies.

12. *Auditing and Oversight*: what mechanisms will be implemented to ensure the Surveillance Technology Specification Report is followed, including what independent persons or entities will be given oversight authority, if and how regular audits will be conducted, and in the case of the Detroit Police Department, also how the Board of Police Commissioners will be involved in the auditing and oversight process.

DPD Response: The Detroit Police Department submits weekly and annual reports to the Board of Police Commissioners.

13. *Training*: what training requirements will be required in connection with the use of the surveillance technology. What qualifications and special skills will be required of persons authorized to use the surveillance technology.

DPD Response: All members will be vetted, CJIS cleared, and trained in all the technology that they are assigned to use. In addition, members are required to comply with Record Retention (101.11), Data Sharing (101.12), Gunshot Detection System (307.8), and all other policies as it relates to technology.

14. *Complaints*: What procedures will allow members of the public to register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the municipal agency will ensure each question and compliant is responded to in a timely manner.

DPD Response: The Detroit Police Department has a policy on Citizen's Complaints (102.6). DPD accepts complaints via e-mail, walk-in, writing and verbal. DPD will continue to adhere to this policy. The Board of Police Commissioners' function is to act as a civilian oversight committee for the Police Department. As such, they have a public comment period for any new policy which would allow for citizens to voice their complaints.