2024 City of Boston Annual Surveillance Technology Report

Camera and Video Management System: Background 2
Boston Police Department 3
Boston Municipal Protective Services, Boston Parks and Recreation Department, Boston Public Schools 10
Department: Boston Municipal Protective Services - Shooter Detection System 16
Boston Police Department - Audio and Video Devices (Recording) 18
Boston Police Department - Audio and Video Devices (Non-Recording) 21
Boston Police Department - Covert Audio and Video Devices 24
Boston Police Department - Automated License Plate Recognition System 27
Boston Police Department - Body Worn Cameras 32
Boston Police Department - Cell-Site Simulator 37
Boston Police Department - Crime Laboratory Unit 41
Boston Police Department - Electronic Intercept & Analysis System ("Wire Room") 46
Boston Police Department - Firearms Analysis Unit 49
Boston Police Department - Forensic Examination Hardware and Software 53
Boston Police Department- Associative Violence Information System (Formerly, Gang Assessment Database) 56
Boston Police Department - GPS Tracking Units 61
Boston Police Department - Latent Print Unit 64
Boston Police Department - Gunshot Detection Technology (SoundThinking ShotSpotter) 68
Boston Police Department - Software and Databases 72
Boston Police Department - Specialty Cameras and Devices (Night Vision, Thermal, Infrared, and X-Ray) 76
Boston Police Department - Unmanned Aerial Systems (UAS) – Drone Technology 79
Boston Police Department - Vehicles Equipped with Surveillance Technology 84
Office of Emergency Management - Critical Infrastructure Monitoring Systems (CIMS) 85
Supplemental Documents 87

Camera and Video Management System: Background

This section describes the structure and general function of the City's camera and video management system, which stretches across multiple City departments. For additional information about how departments use this technology, please review the respective surveillance use policies for BMPS, BPRD, BPD, and BPS.

What is the City's Camera and Video Management System?

The City's camera and video management system includes cameras placed across City property, digital storage infrastructure for captured footage, and the Genetec Video Management System that can be used by authorized staff to see live camera feeds and review archived footage.

What type of data do City Cameras Collect?

Cameras collect video footage within the field of view of the camera. Cameras cannot record audio. Captured video footage is kept for 30 days then automatically overwritten. However, in specific cases, video footage may be kept for a longer period of time. For example, downloaded video footage that becomes part of a BPD Investigation may be kept indefinitely. The following diagram provides an overview of how different City agencies can access cameras and stored video footage.

Department: Boston Police Department
Surveillance Technology: Cameras and Video Management Systems (VMS)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department is dedicated to ensuring public safety in our neighborhoods while balancing civil rights and privacy protections. Video management systems are a tremendous tool for the department in criminal investigations, at large scale events, to protect critical infrastructure, and for other official law enforcement purposes.

For example, the Department's cameras and video management systems may be used to:

- deter criminal activity and public disorder
- reduce fear of crime
- identify criminal activity and suspects
- identify and gather possible evidence for use in criminal and civil court actions
- document police actions
- safeguard citizen and police officer rights
- aid in Amber alerts or in the search for lost/missing children or elderly people
- assist emergency services personnel when responding to incidents
- assist with the monitoring of traffic conditions
- evacuation route status
- monitor transportation networks (airports, waterways, highways, tunnels, transit, intermodal), events and attractions, government facilities, severe weather events
- assist officials with the provision of municipal services in order to enhance overall municipal efficiency
- assist with the training of department personnel.

As of December 31, 2024, BPD's Bureau of Administration and Technology (BAT) maintains a network of approximately 1,400 cameras (the "BAT Camera System") throughout the City of Boston. These cameras are located on fixtures such as light poles, street signs, and buildings. Some of these cameras were purchased and are owned by private entities or neighborhood groups for the purpose of improving safety and security of their business, business district, or neighborhood. These cameras' location and placement was requested by these groups. These groups do not have access to the live stream or recorded video from these (or any) cameras on the BAT Camera System. In early 2024, the Department began to utilize the Genetec Video Management System to view these cameras. None of the cameras owned and operated by the Department have facial recognition or audio capabilities.

The Boston Police Department has direct access to approximately 400 additional cameras that are owned and maintained by the City of Boston (DoIT) and the Boston Transportation Department (BTD) (the "DoIT/BTD Camera System"). The Department uses Genetec to view the cameras on the DoIT/BTD Camera System. The Department has access to view, review, and download video footage.

The Boston Police Department also has direct access to the following cameras via Genetec:

- Approximately 525 cameras owned and maintained by the Municipal Protective Services / City Hall Property Management. The Department has access to view, review, and download video footage.
- Approximately 2,200 cameras owned and maintained by the Boston Housing Authority. The Department has requested that BHA remove access to any interior cameras so access is limited to cameras that show exterior spaces only. Department access is limited to view live video only.
- Approximately 625 cameras owned and maintained by the Boston Public Health Commission. The Department has access to view, review, and download video footage.

The video cameras capture video only ("VMS Video"). The cameras are active twenty-four (24) hours a day, seven (7) days a week ("24/7"). The Department does not monitor the live stream of cameras 24/7.

Cameras on these systems may have pan-tilt-zoom ("PTZ") or thermal capability. Thermal cameras on the BAT Camera System are near water to show heat differential where visibility is reduced.

2. Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.

Please see attached spreadsheet for the 4,138 requests the VEU received in 2024 to provide recorded video from the BAT and DoIT/BTD Camera Systems. These requests for video include both requests made by law enforcement (2,362 requests) and also public records requests (1,776 public records requests).

If the surveillance data is relevant to a criminal case or investigation, all discovery requests or subpoenas made by federal and state prosecutors are directed to the primary investigator assigned to the case. The primary investigator will put in a written request to the VEU seeking a copy of the relevant recordings. The VEU provides a DVD copy of the recording to the investigator who will then provide copies to the prosecutor.

Outside Jurisdictions: Any request for live feed access made by an outside jurisdiction is reviewed for approval through the BPD Bureau of Administration and Technology. If granted, the BPD Telecommunications system administrator will take the necessary steps to activate the connection. If approved, access is granted for a specific time period and only for cameras relevant to the request. This approval and access process will be documented and maintained by the Bureau of Administration and Technology.

Metro Boston Homeland Security Region (MBHSR) Jurisdictions: A jurisdiction within the MBHSR may request archived camera footage from another jurisdiction in the event of a criminal investigation or access to live camera footage in instances such as preplanned major events (i.e., Boston Marathon). In the event that access is granted to an outside jurisdiction, the record of access will be documented and stored to capture the incident number, name of requestor, as well as the location and time of the requested video evidence.

A requesting jurisdiction within the MBHSR will have the ability to view images/video produced by the Critical Infrastructure Monitoring System/VMS cameras only after the BPD has authorized and granted

such access. The Police Commissioner or their designee shall have exclusive authority to authorize other jurisdictions within the MBHSR access to footage recorded by the CIMS/VMS cameras. Access will only include live viewing and/or review viewing (rewinding). It will not include the ability to download or record.

A MBHSR Jurisdiction may also request a copy of archival footage pursuant to the MBHSR CIMS policy.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

On the other hand, the Department continues to receive feedback from the residential and business community requesting additional equipment or expansion of existing technology, including specifically for additional cameras.

For example, at several community meetings held in District B-2, residents requested more public and privately owned video cameras be installed. These residents made these pleas in order to assist the police with solving crime in the business community and their home neighborhoods.

On June 26, 2024, Area B2 participated in Community CompStat at the Dewitt Center inside the Ruggles Development. During this CompStat, residents expressed that they supported the use of technology and how effective it is in solving crimes and reducing fear. As part of the detective's presentation, a case study was presented and investigators explained how the use of residential video was critical in the case being solved.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

Audits: All cameras have audit capabilities via Genetec. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department.

The CIMS project is overseen and managed by the MBHSR Jurisdictional Point of Contact (JPOC) Committee. The Critical Infrastructure and Key Resources (CIKR) Subcommittee will support the JPOC Committee with recommendations based upon subject matter expertise.

In addition, the MBHSR will routinely conduct audits to study funding decisions and their impact in order to better improve the CIMS program and make fiscally sound decisions. To ensure transparency and communication with local governments, the Boston Office of Emergency Management will provide an annual report compiled from audits performed by individual jurisdictions. These reports will identify the number of CIMS cameras within a jurisdiction, the number of users on the network and their permission levels, the number of archived video requests that were approved for footage on CIMS cameras, as well as the number of instances where real-time camera access was granted by a jurisdiction to a requesting agency.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of the cameras or VMS.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Cameras are a tremendous tool for the department in criminal investigations, at large scale events, to protect critical infrastructure and for other official law enforcement purposes. For example:

- Drug Control Unit Officers utilize Department-issued hand held video cameras, the BAT & BTD Camera System and pole cameras (with authorization of a search warrant) to capture real-time interactions that have resulted in search and arrest warrants which will be used in the prosecution of a number of individuals for such offenses that include Trafficking in Heroin and Cocaine.
- In January 2024, Officers responded to a radio call for a commercial burglary at a restaurant in Dorchester. Detectives utilized private video and the BAT & BTD Cameras to track the suspect and an arrest warrant issued.
- In January 2024, Detectives from C-11 and E-5 executed a search warrant at an apartment in Roslindale related to two suspects who were believed to have committed numerous armed robberies (with a Firearm) throughout the City. The investigations were assisted by Body Worn Camera video, the BAT & BTD Cameras, private surveillance video, social media video, electronic product tracking devices, and various Database searches. While executing the search warrant, Detectives recovered stolen property and other evidence connecting the two suspects to eight (8) robberies, including four (4) in Roslindale. Detectives also located a spent shell casing which the Firearms Analysis Unit matched to a shell casing from the scene of one robbery.
- In February 2024, Detectives assigned to District A-1 utilized the BAT & BTD Cameras, along with MBTA and store surveillance video, to identify an individual suspected in two armed robberies of convenience stores in Downtown Boston, which led to his arrest.
- In March 2024, the same suspect robbed three convenience stores while armed with a firearm. The BAT & BTD Cameras were accessed and used to determine the direction of flight after all three of the incidents. Additional private video surveillance systems and security cameras were also used. The suspect was identified and arrested within days of the incidents.

- In April 2024, Detectives utilized the BAT & BTD Cameras and privately owned cameras to identify and locate a suspect in two commercial breaking and entering incidents in Dorchester. The suspect was identified and a warrant issued for his arrest.
- In May 2024, Officers responded to a radio call for a panic alarm at a business in Roxbury. They spoke with the store owner who reported he was robbed at gunpoint when an armed man walked into his store and demanded money. The victim provided a description of the suspect and video from the store. Detectives then tracked the suspect using the BAT & BTD Cameras, which led to the recovery of higher quality video footage from another nearby business. These images were provided to the public via the Office of Media Relations, and Detectives received a tip which identified the suspect, leading to the suspect's arrest.
- In May 2024, Officers responded to a radio call for shots fired in Roxbury. The victim was double-parked waiting for food when two individuals on scooters approached both sides of his vehicle and began shooting at him with his daughter in the backseat of the vehicle. Bullets struck the driver's door of his vehicle and ballistic evidence was recovered from the scene. Detectives utilized the BAT & BTD Cameras to identify the shooters and tracked their movements across the city to a commercial area where higher quality video and images were recovered. Based on these images, Officers identified the suspects and arrests were made.
- In May 2024, two victims suffering from gunshot wounds self-applied to the hospital. Detectives spoke with one of the victims and determined that the shooting took place in South Boston. Detectives were able to review video from the BAT & BTD Cameras and video from the Boston Housing Authority and observed the suspect, his clothing description, and his path of flight after the shooting. This information assisted Detectives in obtaining an arrest warrant for the suspect.
- In June 2024, Officers responded to a radio call for a commercial breaking and entering in Dorchester. Private security cameras and the BAT & BTD Cameras captured the incident and the suspect. Images were disseminated and multiple people identified the suspect and recognized him in relation to other breaking and entering incidents. Detectives secured an arrest warrant and the suspect is facing numerous counts of breaking and entering across the district.
- In June 2024, the BAT / BTD Cameras with GENETEC video management system were used to capture images of two suspects involved in an armed robbery by firearm in Mattapan. The victim reported he was robbed of his iPhone at gunpoint by two male suspects. One suspect was identified and arrested.
- In August 2024, a victim reported that two males on a scooter drove next to her, grabbed her gold necklace from her neck and drove away. BAT & BTD cameras captured images of the two suspects on a scooter who matched the description and who were fleeing in the same direction. After further investigation, arrested warrants were sought for the two suspects in connection with this incident and multiple unarmed robberies across the city.
- In August 2024, Detectives were able to make an identification of a homicide suspect by using private video surveillance footage. Additionally, Detectives were able to trace the path of flight of the suspect, as well as his path to the location of the incident via the BAT & BTD Cameras and MBTA cameras.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.

In 2024, the Department received a total of 6,061 public records requests. The Department received 1,776 public records requests specifically for video from BAT and BTD/DoIT cameras.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.

Between July 2023 and December 2024, the following amounts were spent on cameras:

- $1,227,674 total from UASI funding for CIMS. Of that amount, $923,902 went to supporting cameras in Boston. The number of special events last year required additional staffing, specialized resources, and extended operational hours, all of which contributed to the higher overall cost.

Additionally, during Fiscal Year 2024, the Department spent $141,197 from the Department's Operating Funds, Telecom budget to support cameras maintenance and installations.

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

The Boston Police Department, Brookline Police Department, and Boston Athletic Association entered into a short-term agreement to share live-stream video camera footage during the 129th Boston Marathon. A copy of the agreement is attached.

The Department entered into the attached agreements (Memorandum of Understanding and Procedural Agreement) with the Boston Housing Authority to access video.

Departments: Boston Municipal Protective Services, Boston Parks and Recreation Department, Boston Public Schools
Surveillance Technology: Cameras and Video Management Systems (VMS)

This report consolidates information from each non-BPD department covered by the Surveillance Oversight Ordinance that use cameras (**BMPS, BPRD,** and **BPS**).

Who manages access to each system?

Boston Municipal Protective Services

- The Department Head, Senior Deputy Commissioner, and two Deputy Commissioners manage access to their camera system
    - A limited number of Municipal Protective Services (MPS) officers and alarm operations dispatchers actively use this technology for live monitoring.
    - A limited number of PMD leadership team members may view stored video specifically to respond to a public records request.
    - Two members of the alarm operations section serve as system administrators with the authority to archive select video.

Boston Parks and Recreation Department

- The Director of Park Maintenance, Commissioner, Office Manager, and the Chief of Park Rangers have access to view video footage for cameras that are installed on Park buildings for asset management purposes but are not able to download the footage. The cameras that this group has access to are:
    - George Wright Golf Course
    - Franklin Park Golf Course
    - Deer Park Maintenance Yard
    - Boston Common Maintenance Facility
    - Boston Animal Shelter
    - Canterbury Street Yard
    - Jamaica Pond Boathouse
- Parks staff do not have access to captured video footage nor do they manage access to such footage for cameras that are installed in and around parks.
    - The Parks Department works in partnership with BPD to set up cameras in locations where constituents have requested additional security, but the Parks Department does not have access to live feeds or archived footage.

Boston Public Schools

- Within the BPS Operations Division, the Chief Security Supervisor for the Facilities Management Department is in charge of operating the BPS camera system.

    - Only designated BPS school officials have access to security camera equipment, systems, and recorded footage. BPS employees with access include but are not limited to:
        - the Operations Division including the Deputy Superintendent and Chief Operating Officer
        - Safety Service members
        - School leaders and/or designees,
        - Office of Instructional and Information Technology (OIIT) members for technical support
        - Motorola, an external vendor that provides technical support and troubleshooting
        - Lantel, an external vendor that supports installation
    - The video surveillance network is cloud based. School leaders can only see their school-specific system, not district wide. A single sign on through Google Suite is used.
- No one is actively monitoring live camera feeds during the day
- Video recordings are accessible only to school administrators, officials, or staff directly involved with the content.
    - Recordings used for educational or disciplinary purposes are considered educational records under FERPA.
    - Public event recordings may be released once confirmed to exclude educational or disciplinary content.
    - Parents or guardians can request recordings related to their child's disciplinary matter, subject to privacy considerations.
    - External data requests are reviewed, and if related to a student incident, a subpoena is required, with oversight from the BPS Legal Division.

Capturing Footage from Public Space

Cameras are often positioned in places that capture public space and may capture video footage of members of the public who are not suspected of engaging in unlawful conduct.

For **BPRD** and **BMPS**, security cameras are visible and usually attached to physically elevated infrastructure, like the top of the building or a pole. In these situations, individuals captured on footage are typically able to see the cameras themselves.

BPS adheres to the following guidelines.

- Video footage is kept in the source system to avoid unauthorized access and copies. Duplicating video footage using cell phones or providing someone access to your account <u>is strictly prohibited.</u>
- Video recordings may only be viewed by school administrators, school officials, or school staff members with a direct involvement with the recorded contents of the specific video recording. All access within the system, including viewing live or recorded footage, are recorded.

Recordings that are used for educational, disciplinary, or other related purposes must be treated as an educational record under FERPA.

- Recordings of public events, such as athletics events or public meetings, can be made available to the public after the BPS Legal Advisor or authorized BPS staff designee has determined that the recording does not contain any educational/disciplinary records.
- Parents, guardians, and students over 18 may submit a written request to view video recordings that pertain only to their children/themselves in relation to a disciplinary issue. The viewing may be approved if it does not violate the privacy of other students.
- All external viewing of live or recorded video footage must be approved by the BPS Legal Advisor.

Sharing Video Footage

In the past calendar year:

- **BMPS did not** share any data collected by their portion of the camera system with local, state, federal, or private entities.
- **BPRD did not** share any data collected by their portion of the camera system[1] with local, state, federal, or private entities.
- **BPS did** share data collected by their portion of the camera system. This information is summarized below and included in more detail as appendices.

BPS Data Sharing

The following table describes the number of times video footage was **shared by BPS with another organization in 2024**[2]. It is summarized by the reason data was requested and the recipient. All requests were for one-time data sharing, rather than for ongoing access. For additional detail, please refer to this attached spreadsheet.

Video Footage Recipient	**Reason for Request**	**Number of Times Data Was Shared**
BPS Office of Legal Advisor	Public Records Request	2
BPS Office of Legal Advisor	Subpoena Request	2
BPS Office of Legal Advisor	School Based Incident	1

[1] Requests for video footage captured by BPRD cameras would have been handled by BPD. Please review the BPD's report for their Cameras and Video Management Systems for more information.
[2] This information was not centrally tracked prior to October 2024, but will be recorded moving forward.

BPD	Subpoena Request	1
BPD	Crime in Local Area (Did not involve BPS students or staff)	10
MASS DOT	Motor Accident	1
BPD	Incident that start on BPS site and ended off school property	1
BPS	Bike Theft	1
BPS	Incident Between Student and Admin	1
BPS	On Site Incident During School Hours	1
BPD	Sexual Assault Investigation	1
School Staff	On Site Incident During School Hours	1
School Staff	Property Damage in School Parking Lot	1
	Total	24

Community Input, Public Records, & Audits

Organization	**Public Records Requests in 2024**	**Community Complaints or Concerns in 2024**	**Internal Audits**
BMPS	One (1)	None	None
BPRD	The Parks Department refers public records requests for video footage to BPD, as BPD stores this data	None	None
BPS	Six (6)	BPS facilities received one inquiry into the placement of a camera on an external portion of a building. There were initial concerns that it could capture footage from the neighboring property. After a conversation with the affected people and an adjustment of the	None

		placement, the issue was resolved.	

2024 Funding

Organization	Budget Source	Description	Amount
BMPS	City Operational Budget	PMD Maintenance Contract	$42,251.98
	City Operational Budget	New Cameras	$ 4,193.80
	City Capital Budget		$0
	External Source		$0
	BPRD Total		$46,445.78
BPRD	City Operational Budget	Camera system installation, Canterbury Street Maintenance Yard	$24,296.85
	City Operational Budget	Maintenance Fee for New Installation	$1,000.00
	City Capital Budget		$0
	External Source		$0
	BPRD Total		
BPS	BPS Operational Budget	The BPS Operating Budget supports existing camera infrastructure and maintenance as part of broader technology contracts, but disaggregated expenditures are not readily available.	
	City Capital Budget		$3,481,154.50
	External Source		
	BPS Total		$3,481,154.50

Impact & Effectiveness

BPRD: The cameras installed on City property by Parks are used for asset management. Other cameras in Parks are installed at the request of the community during a community process. These requests

typically come directly in response to destruction of City property, vandalism, graffiti, etc. Installing these cameras directly responds to stated community needs and the process is run through BPD.

- Total number of parks with cameras requested through Parks (All camera installation and data is managed by BPD): **11**

BMPS: The presence of security cameras provide a sense of comfort and safety to employees and visitors. The presence of security cameras also acts as a deterrent to possible criminal activity or vandalism. The cameras also allow for evidence in the event of possible misconduct or criminal investigations.

BPS: Cameras and video management systems improve safety and reduce incidents of violence or disruptions in schools. BPS follows the prioritization lists for camera installations to ensure equity across the district.The prioritization of camera installation in high schools, coupled with the use of a racial equity planning tool, signals an attempt to balance safety and privacy concerns while addressing historical inequities. This approach ensures that racial equity is explicitly considered in the implementation and use of video surveillance. The safeguard of requiring approval from the Legal Advisor for any external viewing or release of live or recorded footage ensures that video surveillance is used in a controlled and responsible manner, mitigating the risk of misuse or over-surveillance. The district's commitment to using video recordings in a way that increases accessibility to school events, improves instructional practices, and enhances operational functions can potentially benefit marginalized communities by providing greater opportunities for participation and learning and ensuring school communities are safe.

The district acknowledges the dual responsibility of maintaining safety while respecting privacy rights, especially in terms of students and families. This approach reflects an understanding that surveillance, like other forms of supervision, must be conducted in a way that protects the privacy of all individuals, particularly those from historically marginalized groups. By addressing both the need for security and privacy, BPS aims to strike a balance that safeguards the well-being of all students, while ensuring that marginalized communities are not subjected to unjustified surveillance that could further stigmatize or harm them.

New Agreements Made in 2024

In the past calendar year:

- **BMPS did not sign any new agreements** with non-City entities related to this technology.
- **BPRD did not sign any new agreements** with non-City entities related to this technology
- **BPS did not sign any new agreements** with non-City entities related to this technology.

Department: Boston Municipal Protective Services[3]
Shooter Detection System

For general information about the Shooter Detection System, what type of data it collects and how it's used, please review the Surveillance Use Policy for the Shooter Detection System.

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

In the past calendar year, this technology was used in a manner consistent with its existing Surveillance Use Policy (summarized above). The system has not been fully activated because no firearm has been discharged on City property covered by the system.

Because this system was not activated by a firearm discharge in 2024, it **did not** capture image, sound, or other information from members of the public who are **not** suspected of engaging in unlawful conduct.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

In the past calendar year, **no data collected by this technology** was shared with local, state, federal, or private entities.

3. **Complaints**: A summary of community complaints or concerns about the Surveillance Technology, if any.

In 2024, Boston Municipal Protective Services (BMPS) received **no community complaints or concerns** about this technology

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

In 2024, BMPS conducted **no internal audits** related to this technology

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

This technology was experimental when first installed. It is designed to activate in a very limited situation, involving an active shooter incident. The technology is designed to be used effectively by

[3] Boston Municipal Protective Services is a sub-unit within the Property Management Department (PMD)

photographing the shooter and notifying the building leadership and Police immediately after a firearm discharge inside City Hall. The City would be able to tell the technology was being used effectively, if it activates immediately after a firearm discharge inside the building.
As effectively as possible in the absence of its activation. We anticipate the technology will be operationally capable this year.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, BMPS received **zero (0) public record requests** seeking documents related to the Shooter Detection system

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

The following table specifies the amount and source of funding for this technology during calendar year 2024 - **no costs were incurred in 2024 by the Shooter Detection System**.

Category	**Organization**	**Amount**
City Operational Budget	N/A	$0
City Capital Budget	N/A	$0
External Source	N/A	$0
Total		$0

BMPS expects this distribution of funding to continue for the foreseeable future.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

Because this technology is exclusively used on City of Boston property and only activated in the case of gunfire on City property, there is no impact on communities of color or other marginalized communities in Boston.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In the past calendar year, **no new agreements** were made with non-City entities related to this technology.

Department: Boston Police Department
Surveillance Technology: Audio and Video Devices (Recording)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

All units of the Bureau of Investigative Services (BIS), the Bureau of Intelligence and Analysis (BIA), Boston Regional Intelligence Center (BRIC), all units of the Bureau of Field Services (BFS), and the Technology Services Division (TSD), Telecommunications Group use audio, video, and audio/video recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The audio, video and audio/video recording devices include, but are not limited to, the following:
- Hand-held audio recording devices (audio only)
- 911 call recording equipment (audio only)
- Cameras recording video at BPD District police stations (in public areas and holding areas) (video only)
- Department issued iPhones (audio and video)
- Audio/video equipment and systems at district stations used for recording witness and suspect interviews (audio and video)

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet for requests the VEU received in 2024 to provide video from cameras at district police stations.

Audio and video data is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints**: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of the audio and video (recording) devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Audio, video, and audio/video recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

The Department received public records requests for 911 calls, text messages and call logs from iPhones, audio and video recorded witness statements, and video recorded from cameras at District police stations. Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Audio and Video Devices (Non-Recording)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Field Services (BFS) and Bureau of Investigative Services (BIS) use video and audio/video non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The following non-recording devices transmit real-time audio and/or video:
- "Throw Phone" with audio and video capabilities used by negotiators to communicate with barricaded individual(s)
- Fiber optic and pole cameras used for officer and community safety in potentially dangerous situations
- Cameras mounted on Boston Police Department vehicles

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Access to the real-time audio and/or video is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were no IAD complaints with an allegation of misuse of audio and video (non-recording) devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The Department uses video and audio/video non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

This technology is used in real-time and does not record.

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Covert Audio and Video Devices

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Bureau of Investigative Services (BIS), Bureau of Intelligence and Analysis (BIA) / Boston Regional Intelligence Center (BRIC), and the Bureau of Field Services (BFS) utilize various covert audio and/or video, recording and non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Data collection capabilities include: (a) non-recording audio, video, and audio/video; and (b) recording audio, video, and audio/video.

Covert audio and video devices shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. *See Commonwealth v. Du*, 495 Mass. 103 (2024); *Commonwealth v. Mora*, 485 Mass. 360 (2020); *see also* BPD Rule 334 (Search Warrant Application and Execution).

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Audio and video data (real-time or recorded) captured by covert devices is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau

of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of covert audio and video devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2024, the Department utilized various covert audio and/or video, recording and non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Automated License Plate Recognition System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Automated License Plate Recognition (ALPR) System in effect in 2024 (3M ALPR System) is a computer-based system that utilizes special fixed cameras to take digital images of a license plate and/or motor vehicle. Boston Police Department Special Order 16-031 (Automated License Plate Recognition System) governs the use of the Department's 3M ALPR System.

The Department's 3M ALPR System captured an infrared image of a license plate and converted it to a text file using Optical Character Recognition ("OCR") technology. Data available in the ALPR System also included the time and geographic coordinates associated with the digital image that was captured. The ALPR cameras did not record video, did not capture sound, and could not be viewed in real-time.

The text file was compared to Vehicle of Interest (VOI) lists generated by law enforcement agencies, including the National Crime Information Center, Massachusetts Department of Criminal Justice Information Services, and the Boston Police Department, to search for a "hit" or potential match. The VOI lists included vehicles that have been stolen, vehicles associated with Amber Alerts, vehicles wanted in connection with specific crimes, and vehicles associated with, or that may assist with the identification of, suspects involved in criminal activity.

During 2024, the Department operated fewer than ten License Plate Readers on the 3M ALPR System. As of April 29, 2025, this equipment is no longer in use and has been decommissioned.

Beginning on April 1, 2025, the Department began a short-term, approximately 90 day, trial of the Flock Safety ALPR System with approximately 45 ALPR cameras. *See* Special Order 25-16 ("Automated License Plate Reader System – Flock System Trial Program").

All ALPR Systems and data are used for legitimate law enforcement purposes and the enhancement of public safety, such as, providing information to officers that will assist in on-going criminal investigations, crime prevention, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and identifying and removing stolen motor vehicles.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet of requests to provide data from the 3M ALPR System received in 2024.

The Operations Division Duty Supervisor may approve a mutual aid request from other law enforcement agencies for use of the ALPR System for purposes consistent with BPD Special Order 16-031, as may be appropriate under the circumstances and as resources permit. Operations Division Duty Supervisors are encouraged to provide mutual aid to other communities when they become aware of a serious incident that they reasonably believe the ALPR System may be useful for. Examples of serious incidents include homicides, shootings, kidnappings, sexual assaults, AMBER alerts, or other serious or violent felonies as to which suspect vehicle information is available.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

Audits: The Boston Police Department Audit and Review Unit is responsible for conducting, reviewing, and retaining audits of the ALPR System usage. Audits shall determine the Department's adherence to Special Order 16-031 as well as the maintenance and completeness of records.

A copy of the audit of the 3M ALPR System conducted on April 29, 2025, is attached.

Discipline: Any employee who engages in an impermissible use of the ALPR System, data associated with the ALPR System, or VOI lists may be subject to disciplinary action up to and including termination. Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the

Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were no IAD complaints with an allegation of misuse of the ALPR System or data.

5. **Effectiveness**: **A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The ALPR System is used for legitimate law enforcement purposes and the enhancement of public safety, such as, providing information to officers that will assist in on-going criminal investigations, crime prevention, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and identifying and removing stolen motor vehicles.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

Additionally, the Department reports the following successful outcomes within the first 60 days of use of the Flock ALPR System:

1. Fugitive Investigation: Units used Flock ALPR to identify a wanted fugitive's vehicle linked to multiple felonies, leading to the suspect's arrest shortly after recognition on the highway. The distinctive license plate images were crucial for identification among many variations.

2. Shooting Investigation: Flock helped identify a vehicle involved in a shots-fired incident believed to stem from a domestic violence situation, providing leads that other cameras could not capture.

3. Larceny Incident: A suspect's vehicle was found using Department video cameras, which revealed an out-of-state plate. Flock's high-quality images and maps allowed detectives to locate the vehicle and identify suspects in areas they frequented.

4. B&E of MV Investigation: In a motor vehicle break-in case, Flock images of an older sedan provided a readable license plate that was not captured by existing Department cameras, aiding in the investigation.

5. Homicide Investigation: Detectives used Flock to input license plate numbers matching the vehicle make and model involved in a homicide case, streamlining the search process and eliminating unneeded manual checks across various locations.

6. Fugitive Investigation: Investigators tracked a vehicle linked to a homicide using Flock. Alerts from the system helped pinpoint areas of frequent sightings, enabling a successful stop and seizure of the suspect vehicle.

7. Kidnapping / Auto Theft Investigation: A victim reported that an unknown suspect jumped into her vehicle, which was occupied by a juvenile, and fled. The vehicle was captured on a Flock ALPR camera which led to recovery of the unoccupied vehicle in the area, the juvenile was located, and the suspect was arrested.

8. Attempted Kidnapping Investigation: Detectives identified a dark sedan with limited identifying information and utilized the Flock System to obtain the vehicle plate, which led to the identity of the suspect and location of the vehicle.

6. Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.

In FY 2024, the Department did not have any expenditures for ALPRs.

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department entered into an agreement with Flock Safety to conduct a short term trial (approximately 90 days) of the Flock ALPR System, which began on April 1, 2025.

The trial includes approximately 45 ALPR cameras and is subject to the following terms, including not limited to:

- All recordings of ALPR data are erased after 30 days unless the BPD requests that data to be retained for legal or investigatory purposes.
- Flock will not share the data.
- Flock will install and maintain its cameras for the agreed upon pilot trial period and all ALPR cameras, and any equipment related to such cameras, will be physically removed from such locations upon the termination of the pilot program.
- The BPD is under no obligation to continue the pilot program or expend any funds for the Flock system during or after the pilot program.
- BPD will not share data (via direct access) with any other agency during the pilot program. External law enforcement requests for information will be handled pursuant to the procedures set forth in SO25-16, Section 11.

Department: Boston Police Department
Surveillance Technology: Body Worn Cameras

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Body Worn Cameras (BWCs) are effective law enforcement tools that reinforce the public's perception of police professionalism and preserve factual representations of officer-civilian interactions. BWCs may be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of incidental evidence or contraband. The equipment will enhance the Department's ability to document and review statements and events during the course of an incident, preserve video and audio information and evidence for investigative and prosecutorial purposes.

BWC recordings, however, provide limited perspective of encounters and incidents and must be considered with all other available evidence, such as witnesses' statements, officer interviews, forensic analysis and documentary evidence. Additionally, studies have shown that BWCs are a contributing factor in reducing complaints against police officers, increasing police accountability, and enhancing public trust.

BWCs and software collect data, images, video recordings, audio recordings, and metadata. BWCs are used with Axon View software.

The Department's Body Worn Camera Policy (Rule 405) was revised January 15, 2025.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet for requests the Video Evidence Unit (VEU) received in 2024 to provide BWC video to law enforcement agencies. The VEU received 7,097 requests in 2024.

Federal, state, and local prosecutors shall make requests for BWC footage directly to the VEU. Pursuant to BPD Rule 405, Sec. 8.1, in accordance with current practice, should an officer receive a subpoena for BWC footage, the officer shall direct the subpoena to their supervisor with a Form 26. The officer shall indicate in their Form 26 that a request for video has been made. The officer shall also direct a copy of the subpoena and Form 26 as soon as practicable to the Video Evidence Unit for response.

Officers are not permitted to provide video to any external partners and shall forward any requests made without a subpoena directly to the Video Evidence Unit.

Upon receipt of the request, the VEU shall determine if the case has been assigned to a detective. If so, the VEU will notify the assigned Detective and/or Detective Supervisor of the request. The Detective or

Detective Supervisor will then be responsible for providing all responsive and related case video directly to the federal, state, or local prosecutor.

If no detective is assigned to the case, the VEU shall identify all relevant BWC footage and provide it directly to the federal, state, or local prosecutor.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

There were no community member complaints about the technology.

The Internal Affairs Division identified potential violations of BPD Rule 405 (Body Worn Camera Policy) while investigating complaints unrelated to the surveillance technology in 15 cases, some of which were complaints initiated by community members. These cases involved the officers' activation of the body worn camera as required by the Rule.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

All Duty Supervisors/Unit Commanders assigned to oversee officers utilizing Department-issued BWCs shall:

1. Ensure officers are utilizing their BWC consistent with BPD Rule 405.
2. Ensure BWCs and related equipment are kept in a secure location within the district or unit.
3. Notify the Video Evidence Unit if an officer utilizes a BWC that is not assigned to him or her, so the Unit may reassign the recordings of audio and video to the officer who created the recordings.
4. Contact the Video Evidence Unit whenever any officer is unable to use the BWC or upload digitally recorded data due to technical problems.
5. Request replacement BWC equipment from the Video Evidence Unit when an officer indicates the equipment is lost or malfunctioning via the Special Notification Form. Once procured by Video Evidence Unit ensure new equipment is received by requesting officer.
6. Ensure that officers include all required references to BWCs in appropriate Department documentation, such as incident reports or Form 26 reports.

Duty Supervisors and Unit Commanders may review BWC data, images, video recordings, audio recordings, or metadata, consistent with BPD Rule 405, to approve any reports.

Audits: Audit and Review conducts periodic checks to ensure Department personnel are using BWCs according to Department policy.

The quarterly audits from 2024 are attached.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 15 IAD investigations that included a potential violation of BPD Rule 405. Each of these allegations are related to officers' activation of their body worn camera.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Body Worn Cameras are effective law enforcement tools that reinforce the public's perception of police professionalism and preserve factual representations of officer-civilian interactions. BWCs are useful in documenting crime and accident scenes or other events that include the confiscation and documentation of incidental evidence or contraband. The equipment enhances the Department's ability to document and review statements and events during the course of an incident, preserve video and audio information and evidence for investigative and prosecutorial purposes.

For example:

- In January 2024, Detectives from C-11 and E-5 executed a search warrant at an apartment in Roslindale related to two suspects who were believed to have committed numerous armed robberies (with a Firearm) throughout the City. The investigations were assisted by Body Worn Camera video, the BAT & BTD Cameras, private surveillance video, social media video, electronic product tracking devices, and various Database searches. While executing the search warrant, Detectives recovered stolen property and other evidence connecting the two suspects to eight (8) robberies, including four (4) in Roslindale. Detectives also located a spent shell casing which the Firearms Analysis Unit matched to a shell casing from the scene of one robbery.
- In March 2024, Body Worn Cameras/Axon VMS System helped the E-18 Detectives hold a suspect responsible for recklessly firing shots in Hyde Park, MA. Shortly after the shooting, Officers in District B-3 stopped the motor vehicle, but the suspect sped off after Officers observed a firearm in the vehicle. Detectives reviewed the Officers' BWC video and matched the suspect's clothing to an individual captured on private surveillance video holding and discharging a firearm in Hyde Park. Additionally, the Firearms Analysis Unit matched ballistics recovered from the scene with evidence thereafter recovered from the motor vehicle.
- In May 2024, Detectives responded to a radio call for a person with a knife in Hyde Park and located a victim who was approached from behind by a suspect who took the victim's cell phone and air pods. Detectives utilized surveillance cameras and observed the suspect had stalked the juvenile victim before the robbery as he walked home from school. In the course of the investigation, Detectives linked this suspect, through surveillance video, Body Worn Camera video, and a fingerprint processed by the Latent Print Unit, to additional incidents including a commercial breaking and entering, larceny of a motor vehicle, and vandalism.
- In June 2024, Officers responded to a radio call in Hyde Park for a person stabbed and located a victim suffering from multiple stab wounds to the back. Witnesses stated there was a group of 15-20 juveniles fighting in the street. An additional victim was also located nearby suffering from a head injury. Due to the severity of the injuries, full notifications were made and Homicide Detectives responded to the scene. Detectives used cell phone video provided to

them, Body Worn Camera video footage, and MBTA surveillance video to identify the juvenile suspect in a near fatal stabbing.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received 983 public records requests for BWC video. In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In CY 2024, the Department spent $5,966,254.

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Cell-Site Simulator

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services (BIS) utilizes a cell-site simulator to locate or identify mobile devices by the device's industry-standard unique-identifying number, such as the International Mobile Equipment Identity (IMEI) number.

The technology is used to locate missing persons, victims of crimes, such as abductions, and criminal suspects. The cell-site simulator is used only for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The cell-site simulator is used (1) with a search warrant obtained after a judicial finding of probable cause; or (2) in exigent circumstances.

Cell-site simulators acquire limited information from cellular devices.[4] Cell-site simulators provide only the relative signal strength and general direction of a cellular device; they do not function as a global positioning locator.

The cell-site simulator cannot collect the contents of any communication or any data contained on the device itself. The cell-site simulator cannot capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an account holder's name, address, or telephone number). Cell-site simulators do not use any biometric measuring technologies.

The cell-site simulator is used in conjunction with vendor-provided software. The associated software displays the location data processed by the cell-site simulator in a format usable by BPD personnel. Data or information will not be retained unless court ordered by a judge.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity,**

[4] Cell-site simulators function by behaving like a traditional networked cell tower. In response to signals emitted by a cell-site simulator, cellular devices within the proximity of the cell-site simulator identify it as the most attractive cell tower in the area. When the simulator is within the cellular device's signal range, it measures the device's signal strength and general direction of the phone. Every device capable of connecting to a cellular network through a cell tower is assigned an industry-standard unique-identifying number by the device's manufacturer or cellular network provider. Cell-site simulators are used either (a) to locate a cellular device where the unique-identifying number is known or (b) to identify a cellular device with an unknown unique-identifying number by deploying the cell-site simulator at several locations where an individual is known to be present and then identifying the unique-identifying number which is present at each of the locations.

the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.

No external entities have access to the BPD cell-site simulator or associated software. This does not prohibit mutual aid or assistance requests by other law enforcement agencies that have been approved by the Commander of the SIU and BIS Command.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

In 2024, the Department received 0 mutual aid or data sharing requests from other law enforcement agencies.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The BPD Investigator or Supervisor requesting to utilize the cell-site simulator must discuss the reasons for deployment with the Commander of SIU and/or BIS Command. Only SIU personnel can operate the cell-site simulator, which may only be done after receiving proper approvals, including a search warrant where exigent circumstances do not exist. A cell-site simulator will not be used without proper internal approvals, even in exigent circumstances.

During 2024, each use of the cell-site simulator followed this protocol.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). The misuse of the cell-site simulator or associated software will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by IAD.

In 2024, neither IAD nor the Commander of SIU received any information regarding misuse of the cell-site simulator or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

In 2024, the cell-site simulator was used 4 times in furtherance of the Department's investigatory, public safety and community caretaking responsibilities. On two occasions, the equipment was used pursuant to search warrants in drug investigations. On one occasion, the equipment was used to confirm the location of a suspect in an aggravated assault incident. On the fourth occasion, the equipment was used under exigent circumstances in an attempt to locate a fourteen year old who had been reported missing / endangered.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of

this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Crime Laboratory Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Crime Laboratory Unit utilizes devices, hardware, and software to provide services including:

- Criminalistics
    - Biological screening
    - General evidence examination
    - Crime scene processing including evidence documentation and collection
    - Bloodstain pattern analysis
    - Footwear comparison
    - Firearms
    - Serial number restoration
    - Gunshot residue - distance determination
    - Shooting reconstruction
- DNA
    - Short Tandem Repeat “STR” analysis
    - Combined DNA Index System (CODIS) – Local DNA Index System (LDIS)
- Trace Evidence
    - Hair/fiber examination
    - Unknown materials testing
    - Primer - gunshot residue testing
    - Polymer and glass analysis

CODIS is a software that serves as a computer database that can be used to generate investigative leads through the comparison of DNA profiles. The CODIS database is connected nationwide at the local, state, and national levels, and primarily consists of two indexes, the Forensic Index and the Offender Index. The Forensic Index contains DNA profiles from casework evidence, and the Offender Index contains DNA profiles from convicted offenders and arrestees. The Boston Police Department Crime Laboratory Unit does not maintain any indices containing Offender Samples or other known individuals.

Through the use of computers and high-speed electronic communications technology, the database can rapidly compare the DNA profiles from casework evidence against each other for any possible “hits,” or matches. This process is valuable to the identification of serial offenders.

The database can also compare the DNA profiles from casework evidence to the DNA profiles from convicted offenders and other known individuals to potentially identify a suspect in a case that previously was unsolved.

The DNA profiles that Crime Lab contributes to the database consist of casework profiles developed from scene samples from unknown individual(s) if the samples and/or profiles meet certain criteria.

Casework samples are analyzed using a minimum of the 13 core STR loci according to procedures described in the DNA Lab Manual. CODIS Eligible evidence from cases without comparison samples are grouped into two categories, or Batches:

SA: Sexual Assault cases

Other: Homicide, Assault and Battery, Breaking and Entering, Car-Jacking, or any non-sexual assault. "Other" batches can occasionally include Sexual Assaults.

For cases processed in a CODIS Batch or without any known reference samples submitted for comparison, an individual Processing Report will be issued to the investigator in charge of the case containing the results of the DNA analyses. The Processing Reports will indicate whether or not a DNA profile was obtained from an evidence item and whether it is suitable for comparison.

The Processing Report will indicate whether the DNA profile will be entered into CODIS software for searching, the level at which it will be searched (LDIS, SDIS, NDIS), and whether further testing is recommended (e.g. Y-STR testing).

DNA profiles for data entry will be technically reviewed by a second qualified DNA analyst prior to entry. The technical review will confirm the data calls as well as the eligibility of the profile for CODIS entry, using the Technical Review Notes worksheets and the CODIS Entry Worksheet.

All DNA profiles entered into CODIS are searched against a local database of Boston Police Department (BPD) casework profiles for possible case to case hits. Qualifying casework profiles are sent electronically to the Massachusetts State Police (MSP) Crime Laboratory for comparison to casework and known (e.g. convicted offender) profiles from across Massachusetts. Casework specimens with data from 6 (or less than 5 with approval) or more core loci meeting Match Rarity Estimate (MRE) can be uploaded to the MSP. The MSP Crime Lab ultimately sends all of the casework with data from 8 or more of the core loci meeting Match Rarity Estimate (MRE) and known (e.g. convicted offender) profiles from Massachusetts to the FBI for comparison to casework and convicted offender or arrestee profiles from across the United States.

The DNA Section Manual, CODIS Manual, Criminalistics Technical Manual, Quality Manual, Trace Evidence Manual, and CODIS Manual can be provided upon request. The publicly available version of the NDIS Operational Procedures manual can be found at the following link: https://ucr.fbi.gov/lab/biometric-analysis/codis/ndis-procedures-manual

2. Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.

The Crime Lab provides any relevant information as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of

specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

Case to case and case to convicted offender/arrestee hits are reported via Hit Notification to the investigator in charge of a case, as well as to the Suffolk County District Attorney's Office. The Hit Notification will contain the identifying information for the case(s), the evidence tested, and the name of the linked individual (if a convicted offender/arrestee or other known hit). Additional information about the convicted offender/arrestee may be listed, such as the social security number or date of birth. This information will vary according to the state jurisdiction that collected the DNA sample from the known offender/arrestee.

A convicted offender/arrestee hit made through CODIS can serve as probable cause to obtain a new DNA sample from the offender/arrestee. The new DNA sample will be processed by the Boston Police Department DNA Section to ensure the accuracy of the DNA match. Upon completion of testing of the new DNA sample from the offender/arrestee, a Comparison DNA Report will be issued to the investigator in charge of the case, as well as the Suffolk County District Attorney's Office, if known.

Data is sent to SDIS (Massachusetts State Police Crime Laboratory) for comparison to casework profiles and convicted offenders from across Massachusetts. Incremental uploads are auto scheduled at a minimum in concordance with the State's searching schedule; uploads can be also sent manually as needed. Full uploads are typically sent as needed, upon notification by SDIS, NDIS or the CODIS Staff (*e.g.*, CODIS Help Desk, etc.).

Data is sent to NDIS for comparison to casework, convicted offender/arrestee, and other known profiles from across the United States. BPD (LDIS) data is sent to NDIS by the MSP (SDIS) only. Samples that meet NDIS acceptance criteria are marked for upload to NDIS at the SDIS level and then forwarded to NDIS for searching. Matches involving BPD data at the NDIS level are automatically sent to the BPD Crime Lab from NDIS and deposited in Match Manager. *See* "Match Manager from SDIS/NDIS Search" section for details on match disposition and reporting guidelines.

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Crime Lab Unit and Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

Audits: The Crime Laboratory Unit is accredited by ANAB (ISO 17025:2017, AR 3125).

A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting November

4, 2024 and ending November 7, 2024. *See* attached BPD Crime Laboratory – ANAB Reassessment Report (Audit Date: November 4, 2024, notification received on February 12, 2025).

Previous ANAB Audits for the CLU can be provided upon request.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

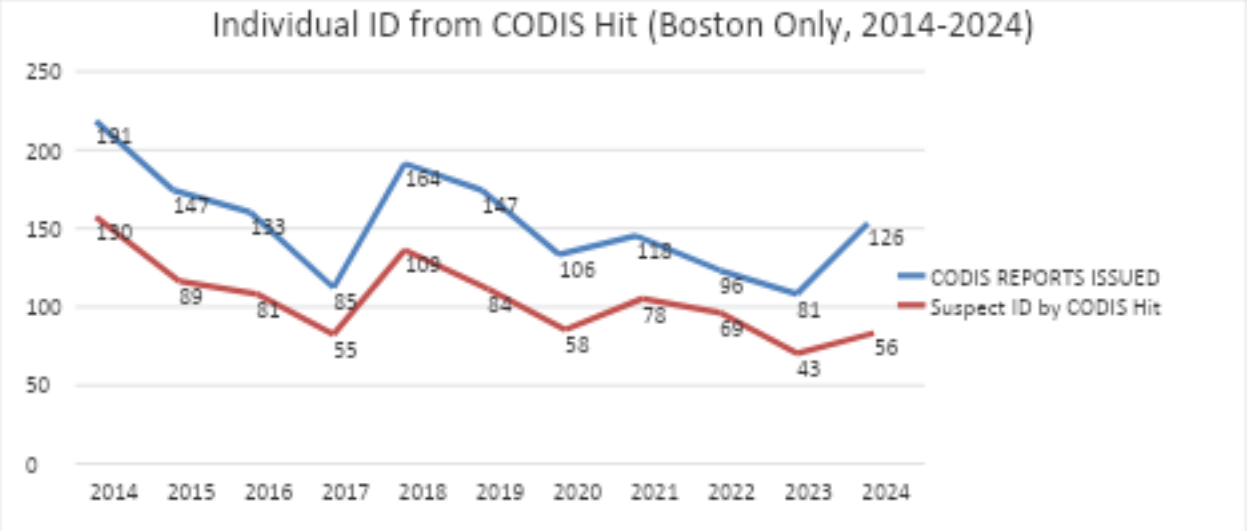
In 2024, there were 0 IAD complaints with an allegation of misuse of the Crime Lab technology or data.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Of note in 2024, two sexual assault cases with no known suspects resulted in a hit; two sexual assault cold cases generated hits, and one homicide cold case resulted in a hit.

Additionally, in the past ten years, an average of 61% of the CODIS Hits have identified an individual, providing investigative information in the case. (53% in 2023 and 44% in 2024).

In 2024, CODIS Hits generated investigative leads through Case-to-Case Hits or Case-to-Offender/Arrestee Hits for 145 cases. (77 in 2023).



2024 CODIS stats for the CLU:

	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Total
Profiles Entered into CODIS	14	22	22	15	37	22	10	12	4	13	11	1	183
Profiles Deleted from CODIS	1	0	2	0	1	0	0	0	0	1	1	1	7
Total Profiles in CODIS	4428	4449	4471	4486	4522	4544	4554	4566	4570	4582	4592	4593	
CODIS Reports Issued													
Case to Case Hits	0	2	4	2	6	8	3	2	2	7	5	4	45
Case to Offender Hits	5	3	11	13	11	16	9	4	7	9	7	5	100
Suspect ID by CODIS Hit	0	2	6	8	9	5	3	2	4	7	8	2	56

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests. The Department received 1 public records request specifically regarding the CLU.

However, public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The technology utilized by the CLU does not have any dedicated personnel cost.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Electronic Intercept & Analysis System ("Wire Room")

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services, Special Investigations Unit utilizes an Electronic Intercept & Analysis System (the "System"), colloquially known as a "Wire Room," to gather evidence of a crime and intelligence about suspected criminal activity conducted by an individual(s) or organized group through interception of wire, oral, or electronic communications.

All data and records collected by the System are obtained by a legal demand, such as an administrative subpoena, search warrant, and court order, and pursuant to federal and state law, including, but not limited to 18 U.S.C. § 2518 and G.L. ch. 272, § 99. *See also* BPD Rule 334 (Search Warrant Application and Execution). On occasion, limited records are obtained as a result of exigent circumstances.

Surveillance data collected by the System include wire, oral, and electronic communications. The specific categories and types of data and records that are collected are determined based on the investigation and are enumerated in the search warrant or court order with the requisite articulation of the probable cause in support of collecting the data pursuant to 18 U.S.C. § 2518 and G.L. ch. 272, § 99.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Access to the data collected is restricted by federal and state law. Data is only shared if the entity is involved in the specific investigation and pursuant to court order or otherwise required by law.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: Security protocols and internal audits are monitored and managed by the System Administrator.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of the Wire Room.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The Wire Room is used to develop evidence of a crime and intelligence about suspected criminal activity conducted by an individual(s) or organized group through interception of wire, oral, or electronic communications.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements**: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Firearms Analysis Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Firearms Analysis Unit (FAU) utilizes devices, hardware, and software to provide services including:

- Crime scene processing including evidence documentation and collection[5]
- Operational/function testing
- Bullet and cartridge casing comparisons
- Ammunition examination
- Firearm characterization
- Determination of class characteristics
- All cases are entered into the National Integrated Ballistics Information Network (NIBIN)[6] and comparison is performed upon request
- ATF E-Trace system

ATF eTrace is an internet-based system that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center (NTC). eTrace allows for the secure exchange of crime gun incident-based data.

By definition, firearms tracing is the systematic tracking of the movement of a firearm recovered by law enforcement officials from its creation by the manufacturer or its introduction into U.S. commerce by the importer through the distribution chain (wholesaler/retailer) to the first retail purchase. Recovered firearms are traced by Law Enforcement Agencies (a) to link a suspect to a firearm in a criminal investigation; (b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; (c) to detect in-state, interstate, and international patterns in the sources and kinds of gun crimes.

Information obtained through the tracing process is utilized to solve and/or enhance individual cases and to maximize investigative lead development through eTrace.

Registered eTrace users can also generate various statistical reports regarding the number of traces submitted over time, the top firearms traced, the average time-to-crime rates, and more. These reports provide a snapshot view of potential firearm trafficking indicators.

The data consists of firearms trace requests, firearms trace results, purchaser, possessor, associate, vehicle and recovery information is captured. This can include an individual's date of birth, place of birth, name, address, height, weight sex, vehicle ID information, driver's license information, recovery

[5] FAU uses BEAST (Bar Coded Evidence Analysis Statistics and Tracking) software program which provides Forensic Laboratory Information Management Systems (LIMS) for case management and tracking. The system is included within the Department's list of "Software."

[6] NIBIN and Integrated Ballistics Identification System (IBIS) are used to match ballistic evidence with other cases. Data uploaded to these systems includes test fires with firearms information; no information is identified with an individual.

information, firearms description, Federal Firearms Licensee information, requesting agency information, officer name and contact information, and special instructions.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

FAU examiners enter information about seized firearms into the eTrace database. ATF may only disseminate firearm trace related data to a Federal, State, local, tribal, or foreign law enforcement agency, or a Federal, State, or local prosecutor, solely in connection with and for use in a criminal investigation or prosecution; or a Federal agency for a national security or intelligence purpose.

FAU provides any relevant eTrace report(s) as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The Firearms Analysis Unit is accredited by ANAB (ISO 17025:2017, AR 3125).

A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting November 4, 2024 and ending November 7, 2024. See attached Firearms Analysis Unit - ANAB Reassessment Report (Audit Date: November 4, 2024).

Previous ANAB Audits for the FAU can be provided upon request.

Internal Audits: Management reviews are conducted annually in the Firearms Analysis Unit. At the advisement of previous assessment teams, the outcomes of management reviews are forwarded to the Command Staff. Internal unit-wide audits are conducted annually in the Firearms Analysis Unit.

External Audits: Full assessment every four years in the accredited units. Surveillance audits every year, with the exception of full assessment years.

eTrace Auditing: The auditing is accomplished on the Oracle database recording the information activity within the database. Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. Audit trails are also used as online tools to help identify problems other than intrusions as they occur.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of firearms analysis unit technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The technology utilized by the FAU does not have any dedicated personnel cost.

8. Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Forensic Examination Hardware and Software

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Electronic Crimes Investigators assigned to the Boston Police Department Forensic Group utilize hardware and software to conduct forensic examinations of handheld devices, computers, and other electronic equipment, including:

- Mobile devices - Smartphones, Tablets, etc.
- Storage devices - Thumb Drives, External Hard Drives, SD Cards/MicroSD
- Computers - Macintosh and Windows
- Network Intrusion Response/Malware Analysis
- Vehicle System Forensics - Infotainment and Telematics Systems
- Skimmer Forensics
- Drone Forensics

Investigators also utilize tools to provide support for Cyber Crime Investigations.

The tools have the potential to access a wide range of data on digital devices, including personal and sensitive information. The data retrieved using the tools and software includes computer files, e-mails, contacts, digital images, audio and video files, and other multimedia files.

All forensic examinations are conducted in furtherance of legitimate law enforcement purposes. Examinations are conducted in criminal investigations with consent or pursuant to a court order. *See* BPD Rule 334 (Search Warrant Application and Execution). Examinations may also be necessary in exigent circumstances. The Department does not use any "[t]ools, including software or hardware, to gain unauthorized access to a computer, computer service, or computer network" -- or any electronic device.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

No other agency has direct access to BPD forensic hardware/software or associated surveillance data. This does not prohibit mutual aid or assistance requests by other law enforcement agencies. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail. When the data extraction/examination forensic tools and software have embedded audit features, the Department shall conduct audits as it deems necessary to ensure appropriate use of the forensic tools and software.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of forensic examination hardware or software.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Electronic Crimes Investigators assigned to the Boston Police Department Forensic Group utilize hardware and software to conduct forensic examinations of handheld devices, computers, and other electronic equipment in furtherance of legitimate law enforcement purposes.

The tools are used to process data important to a wide variety of investigations. Tools that unlock and acquire data from devices are important to Homicide Unit, Sexual Assault Unit, Crimes Against Children Unit and other units and agency investigations. Once the data is acquired, additional tools parse the data into a readable format for investigators to review. All of the tools are used on devices examiners have legal permission to access.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Associative Violence Information System (Formerly, Gang Assessment Database)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Boston Police Department Rule 335 with revisions implemented by Special Order 25-19, effective May 1, 2025, and the Boston Regional Intelligence Center (BRIC) Privacy, Civil Rights, and Civil Liberties Protection Policy (2024), govern use of the Associative Violence Information System, formerly Gang Assessment Database. Following the May 1, 2025 Special Order, the database was renamed the "Associative Violence Information System" to better reflect the types of information stored and functionality.

The Associative Violence Information System is used to:

1. Provide law enforcement a consistent citywide framework for identifying individuals and groups that are reasonably suspected of engaging in criminal activity in furtherance of the criminal group, which includes targeted and/or retaliatory violence; and
2. Assist in the investigation of group related criminal activity in the City of Boston; and
3. Through community-based partnerships, assist in the identification of individuals to be referred to social service partners and offered a variety of opportunities as a pathway out of criminal involvement.

The Associative Violence Information System does not capture images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.

Overall, 71% of individuals in the system have a prior firearm related arrest in Boston.

Associative Violence Information System victim, offender and criminal history statistics:

- Approximately one quarter of one percent (0.25%) of the City's population is represented in the System.
- Approximately 27% of the individuals arrested for firearms offenses in 2024 were in the System.
- Over the last 5 years, an average of 35% of shootings victims were in the System.
- 96% of the individuals in the System have been arrested for a criminal offense in Boston.
- 98% of the individuals in the System have a criminal history in or outside of Boston.

Following the 2021 revision to BPD Rule 335, 2,491 individuals have been deleted from the System through 12/31/24.

- In 2024, 67 individuals were added to the BPD Associative Violence Information System and 169 individuals were removed from the BPD Associative Violence Information System in accordance with the procedures detailed in BPD Rule 335. Additionally, in the spirit of increased transparency, we can report that at the start of 2025, there were 1,704 individuals and 79 groups represented in the Associative Violence Information System.

- In 2023, 111 individuals were added to the System; 161 individuals were purged from the System.
- In 2022, 167 individuals were added to the System; 1,836 individuals were purged from the System.
- In 2021, 59 individuals were added to the System; 609 individuals were purged from the System.
- This info is posted publicly here: https://police.boston.gov/bpd-rule-335-annual-report

The System includes Violent Group Associates and Violent Groups, as defined in BPD Rule 335, and copies of supporting documentation for all criteria used to verify an individual and enter them in the System. The BRIC analyzes the validity of the supporting documentation for each individual criteria used to verify an associate and maintains the discretion to decline to use the information towards any criterion. The BRIC maintains the discretion to *decline* to enter individuals into the System who meet the 10 point criteria but are determined to not be engaged in gang-related criminal activity.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

The information in the System is considered Law Enforcement Sensitive and is thereby For Official Use Only. Its use is limited to the law enforcement community to assist in the prevention, investigation, and resolution of criminal activity. The release of this information beyond these restrictions is strictly prohibited and may constitute a violation of BPD Rules and/or G.L. ch. 268A, § 23. In addition, unauthorized or improper disclosure and/or receipt of this information may impact ongoing investigations or improperly disclose witness identity information, and thereby compromise officer safety as well as that of the public.

Specific Authorized Users within the BRIC, selected by the Commander of the Bureau of Intelligence and Analysis (BIA) or his/her designee will have access to print Gang Associate profile pages / face sheets for legitimate law enforcement purposes. All printing from the System shall be logged and the reason and recipient noted. Attached please find the print log for 2024.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

The BRIC's Privacy Officer, on behalf of the Privacy Committee, is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the BRIC, including the Associative Violence Information System. Complaints and requests for redress are governed by the BRIC Privacy Policy, Section K.

In 2024, the BRIC responded to 1 redress request; the individual was not included in the Associative Violence Information System.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits:

Use/Access Audits: The BRIC maintains an audit trail of accessed information from the Associative Violence Information System. An audit trail will be kept for not more than five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

System Audits: Following revision to BPD Rule 335 in 2021, the System underwent audit and review of all existing individuals to ensure compliance with updates to Section 4.2 ("Gang Associate"), Section 5 ("Gang Associate Verification"), and all individuals meeting the definition of "Juvenile" in Section 4.12 to ensure compliance with Section 10 ("Juveniles"). Additionally, audit and review was conducted of all existing individuals in the System to ensure compliance with updates to Section 9 ("Review of Gang Assessment Database Entries"). This included review of all persons who were entered into the Database more than 5 years prior to the present date to determine based on additional information whether they remain in the "Active" status, per the definition in Rule 335, or will be purged from the Database. Audit and review is ongoing for all persons in the Database: all entries in the Database are reviewed at least every 5 years to determine whether they continue to meet the criteria for inclusion under BPD Rule 335, and juveniles who are included in the Database are reviewed every year.

Following the 2021 revision to BPD Rule 335 (Gang Assessment Database, dated July 8, 2021), 2,491 people have been deleted from the System through December 31, 2024. In 2024, 64 individuals were added to the System; 169 individuals were purged from the System.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). In 2024, there were 0 IAD complaints with an allegation of misuse of the Associative Violence Information System.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Group related violence is impacting neighborhoods in Boston. Intelligence driven community policing is the only way to combat this pervasive issue. As the name suggests, this model starts with intelligence. The intelligence and analysis provided by the Boston Regional Intelligence Center is essential in directing department resources and guiding investigations.

The Associative Violence Information System is one tool that aids the BRIC in providing analysis to drive operational decision making as well as providing real time information in wake of violent events. The tool also allows all officers to have a a consistent citywide framework for identifying individuals and groups that are reasonably suspected of engaging in criminal activity in furtherance of the criminal group, which includes targeted and/or retaliatory violence; and assists in the investigation of group related criminal activity in the City of Boston.

The System is only used for valid law enforcement purposes, including enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of gang related crimes.

For example:

- In May 2024, there was a person shot in the area of Dudley St. Witnesses provided Detectives a suspect description, possible first name of the suspect, and the direction the suspect came from prior to the shooting. An image of the suspect was disseminated by the BRIC to area law enforcement partners for possible identification. Four officers identified the suspect to Detectives based on the image, and Detectives used the Associative Violence Information System to confirm the suspect's identity, their association with a violent group that has participated in violence in the city, and the suspect's history with firearm activity. The suspect was arrested approximately one week after the shooting.

- In July 2024, there was a person shot in the area of Columbia Rd. Detectives spoke to witnesses who relayed information about the suspect who is known by a nickname. Through the course of the investigation, Detectives identified a person of interest who was in the area at the time of the shooting. Detectives then used the Associative Violence Information System and confirmed the person of interest was known by an alias that matched the witnesses' statements. Ultimately, an arrest warrant was sought in connection to this shooting.

- In November 2024, Officers responded to a call for shots fired in the area of Annunciation Rd. Ballistic damage was recovered and an image of the suspect was captured on Boston Housing Authority surveillance cameras. The image was disseminated to area law enforcement partners through the BRIC for possible identification, and two officers contacted the Detective with a possible identification of the suspect. The Detective then utilized the Associative Violence Information System to confirm the suspect's identity and noted this individual was affiliated with a violent group known to participate in previous firearm violence. Ultimately, an arrest was sought for the individual.

Additionally, the System has proven effective in identifying at risk individuals in order to connect them with services. One example of how the System is used to support referrals for services can be found in a situation where, recently, a young juvenile was observed congregating with several significantly older individuals. These individuals are verified associates of a violent group that have participated in firearm violence in the past and their involvement in this violent group was confirmed using the Associative Violence Information System. It is also known that violent group recruitment of young juveniles has been a concerning trend over the last several years. Based on that information, and in an effort to divert the young person from criminal activity, they were referred for services.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing. BPD Rule 113A (Bias-Free Policing Policy).

The Department maintains that no civil rights and liberties have been impacted as a result of its use of the Associative Violence Information System. The Department recognizes that the Associative Violence Information System has been criticized as a dataset that predominantly contains people of color. This unfortunate disparity is due to the gang dynamics in the City of Boston and not as a result of any racially biased practices.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: GPS Tracking Units

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Field Services, Bureau of Investigative Services, and Bureau of Intelligence & Analysis utilize Global Positioning System (GPS) trackers to track the movements and precise location of vehicles, cargo, machinery, and/or individuals. GPS trackers are used for legitimate law enforcement purposes only, and primarily, the investigation of criminal activity, including, but not limited to, investigations into sophisticated drug trafficking organizations, human trafficking investigations, and investigations into organized crime and violent street gangs.

GPS trackers only transmit encrypted data (*i.e.*, movement tracking and location data), which allows authorized BPD personnel to monitor the device's location in real-time. GPS tracker data is also electronically recorded and stored in individual case files.

GPS trackers shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. Consistent with Article 14 of the Massachusetts Declaration of Rights, a warrant application seeking to install a GPS device on a target vehicle, must establish "probable cause to believe that a particularly described offense has been, is being, or is about to be committed, and that GPS monitoring of the vehicle will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense." *See Commonwealth v. Connolly*, 454 Mass. 808, 825 (2009); *see also* BPD Rule 334 (Search Warrant Application and Execution).

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

No outside agencies (City or non-City entities) have direct access to the Department's GPS data.

GPS data is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to, Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court

order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of GPS tracking devices or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

GPS trackers are used for legitimate law enforcement purposes only, and primarily, the investigation of criminal activity, including, but not limited to, investigations into sophisticated drug trafficking organizations, human trafficking investigations, and investigations into organized crime and violent street gangs.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Latent Print Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Latent Print Unit (LPU) uses devices, hardware, and software to provide services including:
- Crime scene processing including evidence documentation and collection
- Latent print processing
- Latent print comparison
- Fingerprint Database searches via two ABIS systems

Automated Biometric Identification System (ABIS) is a tool used to search unknown latent prints found at crime scenes or recovered from evidentiary items against a database of known fingerprints of individuals. Searches of fingerprints/postmortem prints of unknown deceased individuals is an additional service provided by the LPU. The database provides access to known print records for comparison purposes.

The LPU has access to two ABIS database systems:
- MORPHO/Idemia: State database that contains Massachusetts ten print and palm print records. The database was implemented in June 2013 and identifies the candidate list by a State Identification (SID) Number. This database contains both civilian and arrestee records.
- Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) (accessed through the state Morpho/Idemia database): Federal database that contains federal ten print and palm print records. The database identifies the candidate list by FBI number. This database contains both civilian and arrestee records.

ABIS databases may be utilized by the Criminalist to search latent prints when one or more of the following criteria is met:
- No suspect(s) information is available
- Elimination exemplar prints are provided, and no identifications are made
- A request is made by the Investigator
- Criminalist discretion

A Criminalist (original or verifier) may also utilize ABIS databases to assist in a closed search of a latent print(s) with a subject or multiple subjects. When a verifier performs a closed search, the following should be completed:
- Creation of a case in the database to allow for the closed search
- A “V” will be added at the end of the case number when the verifier is performing a closed search
- All information will be entered to create the case with the verifier’s own calibrated image

The Criminalist shall have the authorization to perform or not perform database searches on a case-by-case basis taking into consideration the circumstances of the case and the factors listed below.

A friction ridge impression is suitable for a search when any of the following are present:

- A minimum of 6 clear and unique level two details or higher
- A core and/or delta, or recognizable palm area
- Clarity of detail (may include orientation)

Exigent circumstances may allow for searching of suitable friction ridge impressions prior to complete analysis of all friction ridge impressions in a case.

The LPU also maintains an excel spreadsheet that lists all inked major case impressions being stored in the Forensic Division. Cards are filed by name or criminal record number (CR#). These cards are not considered evidence and copies/representations are retained within the case record as documentation.

Standard Operating Procedures Manual, AFIS Workflow, Mideo Workflow, and Quality Manual include additional information on how the Latent Print Unit utilizes the ABIS databases and can be provided upon request.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Signed reports are retained in LIMS and a copy of the completed report is made available to the Investigator(s). The LPU may provide the District Attorney's Office with a copy of an analysis report upon request by the Assistant District Attorney assigned to the case. In some circumstances, upon verification of a hit performed by a trained and qualified Criminalist, a verbal or written notification of the results can be disseminated to the Investigator prior to the final report. This will be documented in the case record.

The LPU provides any relevant information as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Latent Print Unit and the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The laboratories of the Boston Police Department Forensic Division are currently accredited to ISO/IEC 17025:2017 and ANAB 17025:2017 Forensic Science Testing and Calibration Laboratories Accreditation requirements (AR3125).

A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting November 4, 2024 and ending November 7, 2024. *See* attached BPD Forensic Division – Latent Print Unit ANAB Reassessment Report (Audit Date: November 4, 2024, notification received on February 12, 2025).

Previous ANAB Audits for the LPU can be provided upon request.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of LPU technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

The addition of an ABIS section in the LPU team has been instrumental in utilizing the ABIS databases effectively as reflected in the statistics listed below. The ABIS section has completed a review of all 2016 through 2019 unsolved homicide cases to determine if additional searches could be performed in those cases.

2024 ABIS stats for the LPU:

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	
Latents to AFIS (Local, State, Federal):													
Number of Latents Submitted:	73	78	93	75	87	88	172	52	84	35	57	71	**965**
Number of Searches:	76	89	100	76	96	92	184	55	94	43	63	76	**1044**
Number of Cases:	25	25	23	28	33	28	25	18	21	15	20	33	**294**
Number of ID/Hits:	22	15	9	41	41	19	53	21	24	11	22	28	**306**
Number of Cases with ID/Hits:	11	13	7	12	17	10	12	11	10	6	11	18	**138**

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests; the LPU did not specifically respond to any public records requests.

However, public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The technology utilized by the LPU does not have any dedicated personnel cost.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Gunshot Detection Technology (SoundThinking ShotSpotter)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The City of Boston is an existing end-user customer of SoundThinking's ShotSpotter gunshot location and detection system, which is provided on a software as a service, subscription basis.

The acoustic sensors capture audio recordings of gunshots or suspected gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data is used to locate the incident and is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot.

The sensors are triggered and an incident is created only when 3 or more sensors hear the same loud impulsive sound and can verify a location. This creates an incident and sends a short audio snippet to the ShotSpotter Incident Review center. The snippet includes the gunfire and 1 second of audio prior to and after the gunfire to establish an ambient noise level. Audio clips are typically only a few seconds long.

Real-time notifications of gunfire incidents include the following data: incident location (dot on the map); type of gunfire (single round, multiple round); unique identification number; date and time of the muzzle blast (trigger time); nearest address of the gunfire location; number of shots; district identification; and beat identification. The real-time notification also includes a link to the audio snippet, which is valid for 24 hours.

No personally identifiable information is associated with a real-time notification.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

On the contrary, the Department continues to receive feedback from community members who do not have ShotSpotter coverage. Residential and business community members have requested additional ShotSpotter coverage in more neighborhoods throughout the City.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

The Department publishes datasets regarding confirmed shots fired and persons shot.

Confirmed Shots Fired:
https://boston.hub.arcgis.com/datasets/dd3a722ccc964876b0c6f426541d704d/explore

Persons shot: https://boston.hub.arcgis.com/datasets/boston::person-shot/explore

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of the ShotSpotter system or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

ShotSpotter serves as an acoustical technology that precisely locates the area where gunshots have been fired and provides immediate alert/notification. On average, notifications arrive one to two minutes before 911 calls.

For example:

- In October 2024, Shotspotter activated for 10 rounds in the area of Evans St. A caller reported hearing shots in the area but had no specific additional details. Ballistics were recovered in the area of Evans St. Approximately 10 minutes later, a caller reported a gunshot victim was inside a residence about two blocks from where the ballistics were located.

- In December 2024, Shotspotter activated in the area of Bird St and approximately 4 minutes later a 911 call came in for possible shots in the area of Glendale St, which is a street away from the activation. Ballistics were located at the address the Shotspotter triangulated to.

Sometimes, notifications arrive without a 911 call. This state-of-the-art program and enhanced response time better enables the Department to identify hotspots, recover evidence, and locate victims, witnesses and people in possession of guns.

In 2024, officers responded to ShotSpotter alerts and went to scenes where a victim was shot and there were no corresponding 911 calls in two separate incidents. In one incident, the victim was located when he walked into the Boston Medical Center. ShotSpotter had activated shortly before, but there were no 911 calls. Suspects were identified and arrested. In the second incident, a gunshot victim was located by an officer responding to the area of a ShotSpotter activation where there were no corresponding 911 calls. Ultimately, the victim survived his injuries.

In 2024, similar to 2023, about 40% of confirmed shots fired incidents inside the ShotSpotter coverage zone where ShotSpotter activated did not have a corresponding 911 call. This was calculated by taking the total number of unique gunfire incidents within the ShotSpotter coverage area where a ShotSpotter alert was issued and ballistics were recovered and reviewing whether there was a corresponding, near contemporaneous 911 call to the best of our abilities. The total number of confirmed shots fired in the coverage area without a 911 call was divided by the overall total number of confirmed shots fired in the coverage area (72 / 179).

For example:

- In July 2024, officers responded to a Shotspotter activation in the area of Ashmont St. There were no 911 calls following this activation. Ballistic evidence was recovered and ballistic damage was observed to a parked motor vehicle. RTCC analysts reviewed the cameras in the area of the activation and provided suspect information to officers on scene, detailing clothing, a vehicle description and direction of flight. The vehicle was later located nearby, unoccupied.

- In October 2024, officers responded to a Shotpotter activation in the area of Geneva Ave. There were no 911 calls following this activation. Ballistic evidence was located near Vaughn Ave and a bystander told police they heard what they believed to be two gunshots. RTCC Analysts reviewed the cameras in the area of the activation and relayed information to officers and detectives on scene about a group in the area at the time of the shots fired.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In CY 2024, the Department spent $287,382.00 from the BPD Budget. From February 1, 2024 to January 31, 2025, the UASI grant expended $194,698.00 for ShotSpotter coverage in Boston.

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing. BPD Rule 113A (Bias-Free Policing Policy).

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Software and Databases

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

All Boston Police Department personnel utilize software and databases in the course and scope of their employment to support the administrative and investigatory functions of the Department. Software and databases are used only for valid law enforcement purposes, including, but not limited to, enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of crimes. Additional software and databases are used to support the Department's community service and community caretaking responsibilities.

A detailed, but non-exhaustive, list of software and databases is attached with additional information regarding the data available within the database. This list includes databases maintained by the Department, databases to which the Department contributes data, and databases the Department accesses to view data. The Department also accesses information from publicly available sources, such as social media platforms, including, but not limited to, Facebook, Twitter, Instagram, and SnapChat, and utilizes publicly available applications to improve efficiency in reviewing such information.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. In 2024, the Department did not receive any complaints from the community regarding software or databases.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department.

For databases maintained by the BRIC, the BRIC's Privacy Officer, on behalf of the Privacy Committee, is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the BRIC, including the Associative Violence Information System (formerly, "Gang Assessment Database"). Complaints and requests for redress are governed by the BRIC Privacy Policy, Section K.

In 2024, the BRIC responded to 1 redress request regarding the Associative Violence Information System.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The Department will ensure use of software and databases is in compliance with all applicable laws and regulations. When software or databases have embedded audit features, the Department shall conduct audits as it deems necessary to ensure appropriate use.

The BRIC maintains an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for not more than five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 6 IAD complaints that included allegation(s) of misuse of Department software or databases - in each instance, that an officer improperly accessed or shared CJIS or CORI information. Two complaints had allegations sustained, one complaint was deemed unfounded, and the remainder of the allegations are pending.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

All Boston Police Department personnel utilize software and databases in the course and scope of their employment to support the administrative and investigatory functions of the Department. Software and databases are used only for valid law enforcement purposes, including, but not limited to, enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of crimes. Additional software and databases are used to support the Department's community service and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests. Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

A detailed, but non-exhaustive, list of software and databases the Department utilized in 2024, is attached with additional information regarding the data available within the database.

Software and databases the Department acquired in 2024 include:

- BLTN
- idiCORE

- KACE
- MAAS 360 MDM
- NetMotion
- P3Tips
- PowerDMS
- Sexual Offender Registry Information System (SORIS)

Department: Boston Police Department
Surveillance Technology: Specialty Cameras and Devices (Night Vision, Thermal, Infrared, and X-Ray)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services (BIS), Special Investigations Unit (SIU) and Bureau of Field Services (BFS), Harbor Unit, SWAT, and Special Operations, and Technology Services Division (TSD), Telecommunications Group utilize various specialty cameras and devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Specialty cameras and devices shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. *See also* BPD Rule 334 (Search Warrant Application and Execution).

The specialty cameras and devices include the following:
- Night vision cameras: still photographs or real-time video, non-recording
- Night vision monocular: optic, not a camera
- Thermal imaging cameras: still photographs of recently discarded items, such as firearms; the BAT Camera System (*see* Boston Police Department Cameras and Video Management Systems) is equipped with thermal imaging cameras for viewing heat differential in areas such as Boston Harbor
- Infrared cameras: used by the Harbor Unit to search for individuals or items in the water and do not capture still images or record video
- X-Ray devices: still photographs captured by handheld or robot-mounted devices and used to examine suspicious and unattended items to determine whether explosives are present

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Use of the specialty cameras and devices, viewing their images in real-time, and any still photographs or images captured by the devices are shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of

discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2024, there were 0 IAD complaints with an allegation of misuse of the specialty cameras and devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2024, the Department utilized various specialty cameras and devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Unmanned Aerial Systems (UAS) – Drone Technology

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Remotely operated Unmanned Aerial Systems (UAS) can be effectively utilized to provide first responders with critical information in calls for service, emergency situations, or criminal investigations.

The Boston Police Department Bureau of Field Services, Homeland Security Unit safely and efficiently deploys UAS for legitimate law enforcement purposes, including, but not limited to, the following: providing detailed documentation of crime and crash scenes; assisting in searches for lost or missing children; in support of BPD responses to Code 99 Special Threat Situations, as defined in BPD Rule 200 (Critical Incident Management); and in preparation of large-scale events with significant public safety concerns.

The Bureau of Investigative Services, Crime Scene Response Unit utilizes drones in aerial photography of crime scenes and accident reconstruction.

The Office of the Superintendent-In-Chief, Office of Multi-Media Productions has one UAS that, to date, has not been used. Once the drone is registered, it will be used for public relations and training purposes only. It will not be used for criminal investigations, and it will not be deployed in a manner that allows it to record any personal identifying information.

Additional Drone Detection Technology provided by “DeDrone by Axon” includes “Dedrone City” software and “DJI Aeroscope” sensors utilized by the Bureau of Intelligence and Analysis, Boston Regional Intelligence Center. The system passively monitors for DJI brand UAS operating in the region and has the ability to set up alerts to detect UAS flight within a geofenced zone, such as an area surrounding critical infrastructure. The system can be actively monitored during large scale, high risk special events, major dignitary visits, or as needed based on threat intelligence. The system provides the geographic coordinates of the UAS (including, height, direction of flight and speed), location of the pilot, and serial number of the drone. No personal identifiable information is collected by the system and a search warrant is required to identify the registered owner of the UAS through the serial number of the UAS. DJI brand UAS owners sign a consent agreement when they register their drones prior to use that authorizes monitoring in this manner.

All Department UAS are equipped with individual cameras that have the ability to record video footage. The video footage is recorded on a memory card. If said footage involves a criminal investigation it is transferred, in its entirety, to an external disc or thumb drive.

None of the cameras can record audio. The Department has four UAS cameras that have the ability to view and record with thermal capacity capabilities.

All UAS cameras are used to navigate the UAS as a "first person viewing" camera while it is in flight. Pursuant to the Department's Operations Manual regarding "Protection of Privacy," when a UAS is deployed the onboard camera shall be turned to be facing away from all persons and occupied structures, unless the camera needs to be used solely for the purposes of safely navigating the National Air Space, until the UAS reaches the subject of the deployment.

All UAS must be operated at such an altitude, speed, and with a planned flight pattern, that will ensure inadvertent video recordings or photographs of private spaces of third parties are avoided or minimized. If recording is not necessary during part of, or the entirety of the UAS deployment, such as the camera being used solely for navigation purposes, the Department will not record any video information - it will only be live streamed to the pilot.

UAS shall not be intentionally used for viewing, recording, or transmitting images and/or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless a warrant has been approved for the search of the property, exigent circumstances exist, or the owner or person responsible for the property has given their consent.

All Department UAS pilots are required to properly document all Department flights electronically, via either AirData logbook or, if AirData is not compatible with the UAS, with equivalent software.

A spreadsheet of all 2024 drone flights is attached.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

In 2024, no information was shared and no information was exchanged when UAS were used in conjunction with city agencies and outside local agencies. Information will only be shared with other City Agencies subject to the approval of the Police Commissioner. If approval is granted, the UAS Manager is responsible for coordinating the release of any information to another City Agency.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: A spreadsheet of all 2024 drone flights is attached.

The Boston Police Department UAS Manager is responsible for ensuring UAS annual statistics are saved for all UAS deployments; ensuring that all BPD UAS information that is required to be retained by all applicable laws and ordinances is provided to the Office of the Police Commissioner on an annual basis; and ensuring that all flight and training records are properly maintained by all Department UAS pilots.

All Department UAS pilots are required to properly document all Department flights electronically, via either AirData logbook or, if AirData is not compatible with the UAS, with equivalent software. Training flights are also required to be recorded in either AirData logbook or equivalent software if AirData is not available. This information must be logged after each mission and as soon as practicable.

The UAS Manager is tasked with ensuring all recordings or other information that is gathered as a result of the UAS deployment are properly stored in accordance with Department Rules and Procedures.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). Any officer that uses UAS without proper authorization, deviates from the standards in BPD Rule 407, or violates any other Department Rules or Procedures may be subject to disciplinary action.

In 2024, there were 0 IAD complaints with an allegation of violation of Rule 407 and 0 IAD complaints with an allegation of misuse of drone technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2024, the Department deployed UAS for legitimate law enforcement purposes, including, but not limited to, the following: providing detailed documentation of crime and crash scenes (including aerial

photography and video of crime scenes and accident scenes); assisting in searches for lost or missing children; in support of BPD responses to Code 99 Special Threat Situations, as defined in BPD Rule 200 (Critical Incident Management); and in preparation of large-scale events with significant public safety concerns.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, the Department received a total of 6,061 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request or requests for case investigation files. Due to the broad nature of requests, the responsive documents could potentially include information relative to this technology.

Please see attached addendum re: public records requests.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In 2024, the Department spent $86,927.65.

Information regarding the Department's FY2024 and FY2025 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy24-operating-budget and https://www.boston.gov/departments/budget/fy25-operating-budget. Information regarding the Department's FY2024 and FY2025 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2024, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Vehicles Equipped with Surveillance Technology

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department deploys the following surveillance technology in vehicles:

(1) Cameras, both recording and non-recording
(2) Cell-site simulator

Department: Office of Emergency Management
Critical Infrastructure Monitoring Systems (CIMS)

For general information about the Critical Infrastructure Monitoring System (CIMS) review the Surveillance Use Policy for CIMS.

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

In the past calendar year, this technology was used in a manner consistent with its existing Surveillance Use Policy. This technology did capture images of individuals who are not suspected of engaging in unlawful conduct. The cameras that make up the CIMS network are all located in public places and around critical infrastructure, and it's reasonable to expect that these cameras capture images of people in public near this infrastructure. See Part 2 of the existing Surveillance Use Policy for additional details.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

In the past calendar year, **no data collected by this technology was shared** with local, state, federal, or private entities.

3. **Complaints**: **A summary of community complaints or concerns about the Surveillance Technology, if any.**

In 2024, the Office of Emergency Management (OEM) received **no community complaints or concerns** about this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

In 2024, OEM conducted **no internal audits** related to this technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The identified purpose of this technology is to utilize live video footage during activations of the Emergency Operations Center (EOC) and to maintain situational awareness and a posture of readiness during developing incidents. OEM would rate the effectiveness of the technology at a 5 on a 5-point scale. The system currently provides sufficient situational awareness during developing incidents.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2024, OEM received **no public records requests** seeking documents related to CIMS.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

The following table specifies the amount and source of funding for this technology during calendar year 2024.

Category	**Organization**	**Amount**
City Operational Budget	N/A	$0
City Capital Budget	N/A	$0
External Source	Urban Area Security Initiative (UASI) Grant from FEMA/DHS	~$600,000
Total		~$600,000

OEM expects this distribution of funding to continue for the foreseeable future.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

OEM is not aware of any civil rights and liberties of communities or groups disproportionately affected by the deployment of the Surveillance Technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In the past calendar year, **no new agreements** were made with non-City entities related to this technology.

Supplemental Documents

This publicly-viewable Google Drive Folder contains links for all of the attachments referenced in the above Annual Surveillance Reports.