Table of Contents: Surveillance Use Policies



Appendices: Supporting Documentation

D. BPD Rule 109 (Discipline Procedure)
E. BPD Rule 113 (Public Integrity Policy), as amended/updated by SO 07-016
F. BPD Rule 113A (Bias-Free Policing Policy)
G. BPD Rule 200 (Critical Incident Management)
H. BPD Rule 205 (Death Investigation)
I. BPD Rule 300 (Office of Media Relations – Release of Official Information)
J. BPD Rule 303 (Deadly Force)
K. BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and the Public Record Law (PRL))
L. BPD Rule 322 (Department Property)
M. BPD Rule 322A (Retention and Destruction of Records and Materials
N. BPD Rule 324A (Two-Way Radio and Mobile Data Terminal Procedures)
O. BPD Rule 331 (Digital Images Collection, Transfer & Archive Procedures D.I.C.T.A.)
P. BPD Rule 332 (Suspect Interrogation – Documentation)
Q. BPD Rule 334 (Search Warrant Application and Execution)
R. BPD Rule 335 (Gang Assessment Database)
S. BPD Rule 405 (Body Worn Camera Policy)
T. BPD Rule 406 (Mobile Device Policy)
U. BPD Rule 407 (Unmanned Aircraft Systems Policy Amended)
V. BPD Special Order 16-031 (Automated License Plate Recognition System)
W. BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy)
X. BPD Special Order 21-46 (Outside Agency Notification)
Y. BPD Special Order 22-8 (Video Management System Policy)
Z. BPD Boston Regional Intelligence Center Privacy, Civil Rights, and Civil Liberties Protection Policy (2021)
AA. BPD Data Use Agreement
BB. BPD Latent Print Unit Standard Operating Procedures Manual
CC. BPD Latent Print Unit AFIS Workflow Guide
DD. BPD List of BPD Software and Databases
EE. BPD UAS Operations Manual
FF. Technical Proposal for Subscription-Based Gunshot Detection, Location, and Forensic Analysis Service for the City of Boston (April 28, 2021)
GG. ShotSpotter - Respond Services Agreement
HH. FBI Combined DNA Index System (CODIS) Training Manual
II. BPS Superintendent's Circular LGL-3: Public Records Requests
JJ. BPS Superintendent's Circular LGL-5: Subpoenas
KK. BPS Superintendent’s Circular LGL-7: Privacy of Student Information and Student Record Procedures How to Respond to Student Records Requests in Compliance with FERPA and State Law

LL. BPS Policy Regarding Preparing And Sharing Student Incident Reports And Other Student Information With The Boston Police Department

MM. Metro Boston Homeland Security Region's Critical Infrastructure Monitoring System (CIMS) Policy

**Department: Boston Housing Authority**
**Surveillance Technology: Body Worn Cameras**

1. **Purpose: What's the purpose of this Surveillance Technology?**

Body Worn Camera (BWC) recordings serve as valuable evidentiary tools, and provide a record of encounters between police and civilians that protect the interests and rights of both parties. Additionally, studies have shown that BWCs are a contributing factor in reducing complaints against police officers, increasing police accountability, enhancing public trust and building healthy and productive relationships with the community. BHA purchased the BWC technology in late 2021, but the BWCs have not yet been deployed, as BHA continues to develop its internal policy governing their use. The initial draft policy has been reviewed by an internal committee, including BHA representatives from the bureaus of IT, HR, and community engagement. Policy development is now proceeding in collaboration with BHA residents with support from the BHA community engagement bureau. After this phase of community engagement is complete, the policy will be reviewed by labor unions, general counsel, and the BHA Administrator.

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

Prior to being issued a BWC, officers shall successfully complete training related to the authority's BWC policy and the technical use of the equipment. All department personnel who may supervise officers wearing BWCs or will require access to review videos shall also attend any necessary Boston Housing Authority approved training. Training includes requirements for utilization, activation, notification of recording. uploading and appropriate uses of discretion to protect privacy of minors, among other factors.

When performing any work function, as determined by the Chief of Housing Police or their designee, officers must wear and activate BWCs according to Boston Housing Authority policy, which is in the final stage of development as of July 2022 (the BHA's implementation of BWC was separate from the City of Boston's implementation and the policy is modeled after city protocols). A BHA officer may deactivate the BWC if they determine use of the camera in accordance with the policy and guidelines adopted by the BHA, is appropriate given the sensitivity of an incident, recording of minors, or other relevant factors contributing to their decision.

BWCs will not include technological enhancements including, but not limited to, facial recognition or night-vision capabilities.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

**Department: Boston Housing Authority**
**Surveillance Technology: Body Worn Cameras**

Video and Audio Recording

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

The Chief of Housing Police and Duty Supervisors may access and review BWC footage. Officers may review their own BWC footage when they are involved in an incident, preparing for court, or providing a statement. An Officer requesting to view another Officer's BWC footage or a supervisor requesting to view footage from an officer outside their chain of command shall request permission from the Chief of Housing Police.

Federal, state, and local prosecutors shall make requests for BWC footage to the Chief or their designee. 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, a basic administrative memorandum used by the BPD.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

BWC recordings and data are kept in a secure storage platform managed by the BHA's Network and Video Administrator. Requests for access to footage by users other than an Officer or their Supervisor are routed through the Chief of Housing Police in consultation with BHA legal counsel.

BHA may internally conduct periodic checks to ensure Department personnel are using BWCs according to Housing Authority policy.

6. **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**

The Housing Authority and the Network and Video Administrator will retain BWC footage based on categorization, but may retain all recordings for no less than 180 days, but not more than 30 months, unless the recording relates to a court proceeding or ongoing criminal investigation. The Housing Authority may retain the footage longer on a case-by-case basis as determined by the Chief or their designee. The footage retention schedule for cloud-based footage access is as follows:

**<u>Department</u>: Boston Housing Authority**
**<u>Surveillance Technology</u>: Body Worn Cameras**

Schedule I- Indefinite Retention:
Death Investigation
Code 303- Lethal/Less Lethal discharge of a firearm
Sexual Assault / Abused Person

b. Schedule II- 7 Year Retention:
Use of Force
Arrest
Felony - No Arrest

c. Schedule III- 3 Year Retention:
Misdemeanor - No Arrest
Investigate Person
Investigate Premise

d. Schedule IV- 90 Day Retention:
Significant Event - Public Safety
Traffic Stop
Encounter/FIO
Sick Assist
No Report - Dispatch / On Site

e. Schedule V- 30 Day Retention:
Test/Training

**b) Why is that retention period appropriate to further the purpose(s)?**

Consistent with severity of recorded matter and public scrutiny that may be warranted

**c) What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The system is configured to automatically delete footage after the appropriate time period. Matters subject to indefinite retention will be retained beyond the 30 month period. Footage that has been flagged for a court proceeding or ongoing investigation will be flagged such that it is not deleted

**Department: Boston Housing Authority**
**Surveillance Technology: Body Worn Cameras**

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

The Records Access Officer, or the Chief or their designee shall respond to public information requests submitted under M.G.L. Ch. 66, sec. 10 in accordance with all applicable state laws and regulations.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**

Federal, state, and local prosecutors shall make requests for BWC footage to the Chief or their designee. 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.

    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

BWC Footage related to an Officer Involved Death, Officer Involved Shooting or other Deadly Use of Force will be provided to the Boston Police Department. BPD has automatic jurisdiction over these types of investigations. BPD would generally request the data from BHA in writing, in consultation with general counsel, with the exception of exigent circumstances.

    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

BHA's legal authority and justification to share the subject Surveillance Data may be controlled or limited by the MA. Freedom of Information Act laws and regulations (ref. MGL c. 66A, et seq.; MGL c. 214 § 3B; and 760 CMR 8.00) and/or also by whether the Surveillance Data in question does or does not meet the definition of the state's public record's investigatory materials exemption (ref. MGL c. 4 § 7(26)(f)). See also U.S. Housing and Urban Development Notice PIH 2015-16 (HUD Privacy Protection Guidance for Third Parties).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Training materials will include the policy, technical applications with the device and materials on operation from the BWC manufacturer.

**Department: Boston Housing Authority**
**Surveillance Technology: Body Worn Cameras**

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

The BHA conducts staff training and documents procedures for access to and approval of access requests to use footage. The BHA will periodically review policy compliance through internal audit and will seek to cooperate with external audits by governmental agencies. Additionally, the Chief will assign a supervisory designee to manage the Body Worn Camera program.

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

The following statutes, regulation, and/or legal precedents may be applicable to the subject Surveillance Data and Technology: MGL c. 4 § 7(26) and MGL c. 66 § 1 and 950 CMR 32.00; (MA. Public Record laws and regulation); MGL c. 66 § 1 and MGL c. 30 § 42 (MA. Public Record retention laws); MGL c. 66A, et seq.; MGL c. 214 § 3B; and 760 CMR 8.00 (MA. Freedom of Information Act laws and regulation); Chapter 253 of the Acts of 2020 (An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth); Commonwealth v. Yusuf, 488 Mass. 379, 173 N.E.3d 378 (2021) (the constitutional privacy right implications related to law enforcement use of body-worn cameras); City of Boston Ordinance, Chapter XVI, § 16-63 (Ordinance on Surveillance Oversight and Information Sharing); U.S. Housing and Urban Development Notice PIH 2015-16 (HUD Privacy Protection Guidance for Third Parties); and City of Boston Police Rules and Procedures, Rule 400A (Special Officers-City of Boston or Boston Housing Authority).

11. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

The BHA's BWC directs officers to wear and activate cameras when on duty, but provides discretionary guidelines for deactivation, with notification. The presence of persons who are minors is one of several discretionary guidelines for potential deactivation in order to preserve the privacy of minors.

**Department: Boston Housing Authority**
**Surveillance Technology: Decibel Meter Pilot**

1) **Purpose: What's the purpose of this Surveillance Technology?**

BHA is deploying Decibel Meter in order to understand, detect, and respond to noise and noise complaints made by residents and neighbors of BHA properties. This technology is being piloted in 2022-2023 in partnership with the community as a proactive part of the BHA's response to community concerns around noise and in order to empirically understand noise levels or the frequency of high noise incidents.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

The BHA Chief of Housing Police and Network and Video Administrator will deploy Decibel Meter installations following consultation with BHA's Administrator, residents and neighbors. The decibel meter is a detection system that does not require human activation. The Decibel Meter is not used for the purpose of individual monitoring or for recording or analysis of audio.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

The Decibel Meter sends email and/or text alerts when noise has reached a level prohibited by city ordinance (50 decibels 11PM-7AM and 70 decibels at any time), a certain volume in a given area, but does not record audio. Emails are stored as public record.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

The Chief of Housing Police and their designee(s), who shall include the Deputy Chief of Housing Police and a Housing Police Sergeant charged with overseeing video system requests, may access and review Decibel Meter alerts. The BHA's Network and Video Administrator may access and review Decibel Meter alerts.

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

**Department: Boston Housing Authority**
**Surveillance Technology: Decibel Meter Pilot**

The Decibel Meter does not retain sensitive data. The data it produces, alerts regarding excessive volume in a generalized area, would be public record. That said, the BHA will limit distribution of data to legitimate public purposes.

6) **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b) **Why is that retention period appropriate to further the purpose(s)?**
    c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The Housing Authority will retain records of alerts consistent with requirements under the public records law.

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

The Records Access Officer, or the Chief or his/her designee shall respond to public information requests submitted under M.G.L. Ch. 66, sec. 10 in accordance with all applicable state laws and regulations.

8) **Information and Data-Sharing:**
    a) **How can other City or non-City entities access or use the Surveillance Data?**
    b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

To the extent the BHA agrees to share such data with other agencies, the BHA will develop memoranda of agreement for use or exchange of such data. The BHA may share such data outside the context of a defined memorandum if distribution is necessary in the immediate interest of public safety or other exigent circumstances exist.

BHA's legal authority and justification to share the subject Surveillance Data may be controlled or limited by the MA. Freedom of Information Act laws and regulations (ref. MGL c. 66A, et seq.; MGL c. 214 § 3B; and 760 CMR 8.00) and/or also by whether the Surveillance Data in question does or does not meet the definition of the state's public record's investigatory materials exemption (ref. MGL c. 4 § 7(26)(f)). See also U.S. Housing and Urban Development Notice PIH 2015-16 (HUD Privacy Protection Guidance for Third Parties).

9) **Training:**
    a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

The BHA will train officers, supervisors or staff who it grants access to Decibel Meter Data to understand and describe what such data does and does not signify, and how to utilize such technology without compromising or creating the perception of compromising privacy.

    b) **What are the training materials?**

The BHA will train officers, supervisors or staff who it grants access to Decibel Meter Data to understand and describe what such data does and does not signify, and how to utilize such technology without compromising or creating the perception of compromising privacy.

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

The BHA conducts staff training and documents procedure for access to and approval of access requests to decibel meter data. The BHA will periodically review policy compliance through internal audit and will seek to cooperate with external audits by governmental agencies.

11) **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

The following statutes, regulation, and/or legal precedents may be applicable to the subject Surveillance Data and Technology: MGL c. 4 § 7(26) and MGL c. 66 § 1 and 950 CMR 32.00; (MA. Public Record laws and regulation); MGL c. 66 § 1 and MGL c. 30 § 42 (MA. Public Record retention laws); MGL c. 66A, et seq.; MGL c. 214 § 3B; and 760 CMR 8.00 (MA. Freedom of Information Act laws and regulation); Chapter 253 of the Acts of 2020 (An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth); City of Boston Ordinance, Chapter XVI, § 16-63 (Ordinance on Surveillance Oversight and Information Sharing); U.S. Housing and Urban Development Notice PIH 2015-16 (HUD Privacy

Protection Guidance for Third Parties); and City of Boston Police Rules and Procedures, Rule 400A (Special Officers-City of Boston or Boston Housing Authority).

12) **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

N/A for this technology as the alerts would neither distinguish nor disproportionately impact minors.

**Department: Boston Municipal Protective Services**
**Surveillance Technology: Cameras and Video Management System**

1) **Purpose: What's the purpose of this Surveillance Technology?**

The Property Management Department (PMD) Boston Municipal Protective Services (BMPS) network of security cameras is installed in City Hall, City Hall Plaza, and a variety of other City-owned buildings for security purposes, to maintain a safe environment for City employees and visitors, and monitor outdoor areas around City Hall and other City-owned buildings. Specifically, there are 384 total security cameras installed in 17 locations; 250 of the cameras cover PMD locations and 134 cameras cover PWD, Parks, BFD, and MOH locations but are located in the BMPS security camera partition for convenience and efficiency. BMPS cameras include 163 at City Hall, 22 at Faneuil Hall, 32 at 1010 Massachusetts Avenue, 11 at 95 Magazine Street, 4 at 20 City Hall Avenue, 4 at 43 Hawkins Street, 2 at 41 New Chardon Street, 9 at 201 Rivermoor Street, and 3 at 500 Columbia Road. The non-BPMS cameras include 33 at BFD Headquarters, 58 at 400 Frontage Road and PWD streetlight and fuel locations, 30 at the Parks Department Franklin Park Maintenance Yard and George Wright Golf Course, and 1 at the Strand Theatre.

Security cameras were installed at various times with operating funds and with OEM grant funding with the first cameras installed shortly after September 11, 2001 in City Hall and continuing to date. PMD anticipates continuing to add more cameras in the future. Originally, we installed analog cameras linked to local recorders, but in the last ten years have migrated to digital cameras on a network, currently operating on the Genetec video monitoring system software, which BMPS acquired prior to 2016. 11 older cameras at 201 Rivermoor Street and 1 camera at 43 Hawkins Street, are currently in the process of being migrated onto the Genetec network.

The original video surveillance camera design for the renovated City Hall Plaza included license plate recognition (LPR) cameras to be installed for security purposes, to protect the physical integrity of the Plaza, maintain a safe environment for City employees and visitors, and monitor outdoor areas around City Hall. However, as the design progressed, the LPR capability was not procured or implemented. When the plaza renovation is complete, none of the security cameras will have license plate recognition capabilities. Additional LPR software (Genetec AutoVu) would need to be purchased and programmed before the designated cameras could be configured to recognize and record license plate information.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

The purposes of these cameras are for security purposes, to maintain a safe environment for City employees and visitors, and to monitor outdoor areas around City Hall and other City-owned buildings. Cameras used solely for security purposes or installed solely to protect the physical integrity of City infrastructure are exempt from City of Boston Ordinance 16-63, pursuant to sections 16-63.3(b)(2)(K-M). However, BMPS security cameras have the capability to be used for other purposes, such as following possible misconduct, injury, or criminal activity.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

Cameras are able to collect video footage within the field of view of the camera. Cameras cannot record audio. Footage is retained for 30 days and then automatically overwritten.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Access to our current security camera network is limited to Boston Municipal Protective Service (BMPS) officers and select Department managers. Authority to access to search or export data is restricted and requires authorization from the Department Commissioner, Chief of Staff, Deputy Commissioner, or Chief of Security.

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

Data is encrypted and requires logon authorization and password access control. Only limited personnel have the authority to search or export stored data. The Department contracts with a licensed integrator, Siemens Industry, Inc., to manage the security camera network.

6) **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**

Data will be overwritten after 30 days, unless intentionally saved.

    b) **Why is that retention period appropriate to further the purpose(s)?**

The retention period is subject to available computer storage space. The 30-day retention period allows the Department a reasonable period of time to investigate reports of possible misconduct, injury, or criminal activity. Within the 30 day window, BMPS may save a segment of video data in a storage feature called the vault for a predetermined time or indefinitely. Indefinite storage is discouraged because it uses valuable storage capacity.

    c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

Data is programmed to be automatically overwritten and deleted after 30 days, unless intentionally saved. Authority to retain data after 30 days is restricted to BMPS or Department supervisors or managers.

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

Data can be accessed through the public record request process or court order. BMPS will seek legal guidance prior to allowing public or criminal defendant access to data.

8) **Information and Data-Sharing:**
   a) **How can other City or non-City entities access or use the Surveillance Data?**

See response to 7). MPS will seek guidance from the Law Department for access by non-City entities.

   b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

The information will be shared with the Boston Police Department for investigations through proper channels. The information with non-City entities and organizations will not be shared without Law Department guidance.

   c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

The public record request statute, judicial court order, and/or legal advice from the City of Boston Law Department.

9) **Training:**
   a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

Training is performed by Department personnel including supervisory BPMS officers and our security alarm operations program manager. Training is also provided by our licensed integrator, Siemens Industries, Inc., as needed. Additional training may be provided by the plaza renovation project security consultant.

   b) **What are the training materials?**

New employees learn to operate the video monitoring software with in-house training. The software is intuitive. The Department works closely with DoIT and our integrator, Siemens Industries, Inc. to implement software upgrades. PMD is updating our training materials since the recent enactment of the police accountability law, including updating training materials for the requests for incident reports and surveillance video.

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance**

**with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

Authorization to release video surveillance data will be restricted to Department senior managers. Data will not be released without a written request identifying the requestor or a request through the City's public records request procedure. Sanctions from misuse will include Office of Human Resource and Collective Bargaining Agreement disciplinary processes.

11) **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

BMPS will follow the public records law and City procedure and continue to seek guidance from the City Law Department specific to video surveillance data.

12) **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

BMPS has very limited coverage in the City Hall daycare to protect the privacy of attendees. Otherwise, there are no special considerations for child rights.

**Department: Boston Municipal Protective Services**
**Surveillance Technology: Shooter Detection System**

1) **Purpose: What's the purpose of this Surveillance Technology?**

The Shooter Detection Systems Company Guardian System is intended to identify a potential active shooter with acoustical sensors in 10 locations and 29 cameras in entrance lobbies, the loading dock, Mayor's Office, City Council Chamber, and near large public meeting rooms in City Hall by detecting a firearm discharge and activating surveillance cameras in the specific location of the discharge. The technology was installed with OEM grant funding and installation completion in February 2018.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

In the event of a gunshot or muzzle flash, the technology is designed to immediately create video and still photographs of the specific location and to alert designated building occupants of the location. The system includes the shooter detection sensors that are linked to security cameras. The system has the capability to send alerts by email, SDS messaging, and the building intercom system to notify building occupants of the potential active shooter.

At the current time, the SDS message feature and building intercom system are not enabled. The Department is working with DoIT to review the list of employees programmed to receive email notification.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

Upon activation, video footage is recorded instantaneously; cameras will record the site of the gun discharge. The shooter detection system is programmed to create a log of the local time and date of activation. No data is collected unless the system is activated. Building video cameras overwrite saved video footage after 30 days.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Video footage is collected by our internal video monitoring system. Department managers and select BMPS employees can access video footage. Lan-Tel technicians receive error messages for system malfunctions but can only access the shooter detection log by connecting to our server in the DoIT Data Center. In over four years, the technology has never been activated. Lan-Tel does not receive the video.

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

The shooter detection system data is encrypted by the manufacturer and access to the log is limited to authorized Lan-Tel technicians who would need to access a server in the DoIT Data Center, a restricted area requiring an escort from DoIT. Access to security camera video footage requires log on and password credentials and is limited to Department managers and select BMPS employees. .

6) **Data Retention:**

   a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**

The shooter detection system log is located on a City server and only captures local time and date information if the system is activated. The log time period is indefinite. To date, the system has not been activated since installation over four years ago. Security camera video footage is overwritten after 30 days, unless specifically saved and stored in the video monitoring system vault.

   b) **Why is that retention period appropriate to further the purpose(s)?**

See response to 6) a). The storage of security camera footage also requires a large amount of computer server storage capability.

   c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The video footage is automatically deleted when overwritten after 30 days, unless specifically saved. The shooter detection data log has never been activated or accessed. See also response to 6) a).

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

The data is not accessible by the public, including criminal defendants at this time. Public access would be subject to City protocols for public records requests under state law. Criminal defendants could request access through the judicial discovery process.

Separately, City Hall does have security cameras throughout the building with surveillance video available for 30 days unless saved, and members of the public, including criminal defendants, could request security camera video by public record request or court order.

8) **Information and Data-Sharing:**

**Department: Boston Municipal Protective Services**
**Surveillance Technology: Shooter Detection System**

a) **How can other City or non-City entities access or use the Surveillance Data?**

BMPS would need to request assistance from Lan-Tel to access the local time and date of activation of the shooter detection system log. BPMS would share this information with authorized City Departments. BMPS can access security camera footage up to 30 days until overwritten, unless the footage was saved.

b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

BMPS refers requests for data with non-BPD law enforcement agencies to the Department Commissioner. The Department Commissioner consults with the City Law Department prior to releasing data. The information is not shared. See also response to 7).

c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

Not applicable. See also response to 7).

9) **Training:**
   a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

Department managers are reviewing training procedures with the technology contractor.

b) **What are the training materials?**

The Department is requesting training materials for the shooter detection system from Lan-Tel to train our current employees on the system capabilities and operations. The Department will share training materials with DoIT and OEM and continue to improve building security and safety procedures. System maintenance requires specialized and certified technicians and software licenses.

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

Department managers are continuing to consult with Security Camera Federation partners, including representatives from BPD, OEM, DoIT. The Federation meets to implement best practices in the security camera industry and to standardize technology and procedures among City Departments. Technology access is encrypted with limited access and requires periodic software licensing.

11) **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

The technology has not been activated in more than four years. The Department will consult with the Law Department if release or disclosure is required.

12) **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

There are no special considerations for child rights with this technology.

**Department: Boston Police Department**
**Surveillance Technology: Audio and Video Devices – Non-Recording**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The Boston Police Department Bureau of Field Services (BFS), SWAT, Special Operations Unit, and Youth Violence Strike Force (YVSF) 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 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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Use of audio and video devices shall be limited to only BPD personnel authorized by the Department to deploy the devices in the course and scope of their employment to support the administrative and investigatory functions and community caretaking responsibilities of the Department.

   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 also* BPD Rule 334 (Search Warrant Application and Execution).

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   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

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Real-time audio and/or video may be viewed on an attached monitor(s) or, for some cameras, through the FLIR Video Management System. Access to the real-time audio and/or video shall be limited to authorized BPD personnel for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

   All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

   Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at:

https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Training on the operation of audio and video devices is provided by the vendors or by appropriate Department personnel.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

    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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department audio and video devices shall be deployed and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department audio and video devices shall be deployed and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

**Department: Boston Police Department**
**Surveillance Technology: Audio and Video Devices - Recording**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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 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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Use of audio and video recording devices shall be limited to only BPD personnel authorized by the Department to deploy the devices in the course and scope of their employment to support the administrative and investigatory functions of the Department.

   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* BPD Rule 334 (Search Warrant Application and Execution).

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   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); *see* BPD Rule 324A (Two-Way Radio and Mobile Data Terminal Procedures)

   - Cameras recording video at BPD District police stations (in public areas and holding areas) (video only)

- Department issued iPhones (audio and video); *see* BPD Rule 406 (Mobile Device Policy)

- Audio/video equipment and systems at district stations used for recording witness and suspect interviews (audio and video); *see* BPD Rule 332 (Suspect Interrogation – Documentation)

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Audio and video devices shall be stored in a secure location. All recorded audio, video, and audio/video data collected by the devices shall be stored in the physical case file and/or stored within a BPD-approved electronic case/content management system (*i.e.*, "Detective Case Management"). Access to audio and video data shall be limited to authorized BPD personnel for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
   a. **How can other City or non-City entities access or use the Surveillance Data?**
   b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
   c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Training on the operation of audio and video recording devices is provided by the vendors or by appropriate Department personnel.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

All Boston Police Department audio and video recording devices shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

All Boston Police Department audio and video recording devices shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs,

and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix N: Boston Police Department Rule 324A**
- **Appendix P: Boston Police Department Rule 332**
- **Appendix T: Boston Police Department Rule 406**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The Boston Police Department Automated License Plate Recognition (ALPR) System is a computer-based system that utilizes special fixed cameras to take digital images of a license plate and/or motor vehicle. The ALPR System captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition ("OCR") technology.

   The text file is 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 include vehicles that have been stolen, vehicles associated with Amber Alerts, vehicles wanted in connection with specific crimes, vehicles associated with, or that may assist with the identification of, suspects involved in criminal activity.

   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.

   As of August 1, 2022, the Department operates less than ten License Plate Readers.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Boston Police Department Special Order 16-031 (Automated License Plate Recognition System) governs the use of the Department's ALPR System.

   The ALPR System is restricted to legitimate law enforcement purposes only in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities

The Department shall only use the ALPR System, including adding a vehicle to VOI lists, where there is a legitimate and specific law enforcement reason for identifying a vehicle or a person reasonably believed to be associated with that vehicle.

Only Department employees trained in the use of the ALPR System and BPD Special Order 16-031 may access the ALPR System. Each authorized Department employee is issued an individual log-in identification which allows the user to view the digital images of a license plate along with the data, including time and geographic coordinates associated with the vehicle image that was captured, VOI lists, and any potential hits.

Prohibited uses of the ALPR System include:

1. Invasion of Privacy. Except when done pursuant to a court order, it is a violation of BPD Special Order 16-031 to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (*e.g.*, vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a business establishment).
2. Harassment/Intimidation. It is a violation of BPD Special Order 16-031 to use the ALPR System, data associated with the System, or VOI lists, to harass and/or intimidate any individual or groups of individuals.
3. Use Based on Protected Characteristics. It is a violation of BPD Special Order 16-031 to use the ALPR System, data associated with the System, or VOI lists, solely because of a person's race, gender, ethnicity, sexual orientation, disability, or other classification protected by law.
4. Personal Use. It is a violation of BPD Special Order 16-031 to use the ALPR System, data associated with the System, or VOI lists, for any personal purpose.
5. First Amendment Rights. It is a violation of BPD Special Order 16-031 to use the ALPR System, data associated with the System, or VOI lists, for the purpose of infringing upon any individual's or group's First Amendment Rights.

**3. Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

The ALPR System utilizes special fixed cameras that take digital images of a license plate and/or motor vehicle. Data available in the ALPR System also includes the time and geographic coordinates associated with the digital image that was captured.

The ALPR cameras do not record video and cannot be viewed in real-time.

**4. Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Only Department employees trained in the use of the ALPR System and Special Order 16-031 may operate the ALPR System or access or use stored ALPR data. Each

authorized Department employee is issued an individual log-in identification and is required to utilize alphanumeric password consisting of a combination or upper- and lower-case letters, numbers, and symbols. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   All ALPR data shall be kept in a secure data storage system stored locally on a Department server (not cloud-based) with access restricted to authorized persons only. The ALPR System, associated data, and VOI lists are considered confidential information to the extent permitted by federal and state law and case law. This data is also maintained in accordance with all local ordinances, including, but not limited to, 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

   Scanned data is retained for a period of thirty days and then automatically deleted. Data required for investigatory purposes, evidentiary purposes, by court order, or by law is retained as appropriate.

   All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

   All media requests made related to surveillance data from the Department ALPR System will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

   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.

   All ALPR data requests submitted in connection with open investigations pursuant to a court order, subpoena, or discovery request, are processed through the primary investigator assigned to the investigation through the Technology Services Division. Requests that are not associated with an open investigation are forwarded to the Office of the Legal Advisor and handled in accordance with the applicable federal or state laws.

8. **Information and Data-Sharing:**
   a. **How can other City or non-City entities access or use the Surveillance Data?**
   b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
   c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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 or 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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Department employees must be familiar with Special Order 16-031 before they are allowed to operate the ALPR System or access or use stored ALPR System data. Department employees must also be properly trained on how to use and inspect the ALPR System equipment.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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.

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. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    The Boston Police Department ALPR System shall be deployed, and all data shall be collected, maintained, and utilized, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The Boston Police Department ALPR System shall be deployed, and all data shall be collected, maintained, and utilized, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to *Commonwealth v. McCarthy*, 484 Mass. 493 (2020), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to, Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix V: Boston Police Department Special Order 16-031 (Automated License Plate Recognition System)**

**Department: Boston Police Department**
**Surveillance Technology: Body Worn Cameras**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   BPD Rule 405 (Body Worn Cameras) governs the use of BWCs.

   Officers shall use BWC data, images, video recordings, audio recordings, or metadata only for legitimate law enforcement reasons.

   It is the policy of the Department to respect the legitimate privacy interests of all persons in Boston, while ensuring professionalism in its workforce. Officers shall only use BWCs within the context of existing and applicable federal, state, and local laws, regulations, and Department rules and policies. The Department prohibits recording civilians based solely upon the civilian's political or religious beliefs or upon the exercise of the civilian's constitutional rights, including but not limited to freedom of speech, religious expression, and lawful petition and assembly. BWC footage shall not be reviewed to identify the presence of individual participants at such events who are not engaged in unlawful conduct. BWCs will not include technological enhancements including, but not limited to, facial recognition or night-vision capabilities.

When performing any patrol function as determined by the Police Commissioner or his/her designee, officers assigned BWCs must wear and activate BWCs according to Department policy, including the following sections of BPD Rule 405:

- Section 2.2: Camera Activation and Incidents of Use
- Section 2.3: Recording within a Residence
- Section 2.4: Recording in Areas Where There May be a Reasonable Expectation of Privacy
- Section 2.5: Notice of Recording
- Section 2.6: Consent to Record
- Section 2.7: Recording of Victims/Witnesses
- Section 2.8: BWC Deactivation
- Section 2.8.1: Suspicious Device Protocol
- Section 2.9: Special Operations Division Activation Factors

Officers shall not use BWCs to record in violation BPD Rule 405 or any rule or procedure of the Boston Police Department, including:

1. During breaks, lunch periods, or time periods when an officer is not responding to a call, or when not in service;
2. Any personal conversation of or between other department employees without the recorded employee's knowledge;
3. Non-work related personal activity, especially in places where a reasonable expectation of privacy exists, such as locker rooms, dressing rooms, or restrooms;
4. Investigative briefings;
5. Encounters with undercover officers or confidential informants; or
6. Departmental meetings, workgroups, in-service training, or assignments of an operational or administrative nature.

Additional improper use of BWC footage includes:

1. Officers shall not use data, images, video recordings, audio recordings, or metadata for personal reasons, or non-law enforcement reasons.
2. Department personnel shall not use BWC data, images, video recordings, audio recordings, or metadata to ridicule or embarrass any employee or person depicted on the recording.
3. Department personnel shall not disseminate BWC data, images, video recordings, audio recordings, or metadata unless the Police Commissioner or his/her designee approve the dissemination and the Department personnel disseminates the BWC data, images, video recordings, audio recordings, or metadata in the course of his/her official duties.
4. Department personnel shall not copy or otherwise reproduce any BWC recording/footage (including using an iPhone, iPad, or other electronic or other device).
5. Bureau Chiefs, supervisors and Internal Affairs shall not randomly review BWC recording/footage for disciplinary purposes.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   The BWC equipment and all data, images, video recordings, audio recordings, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the Boston Police Department and shall not be released without the authorization of the Commissioner or his/her designee. *See also* BPD Rule 322 (Department Property).

   Officer Access to Their Own Footage (Not Related to Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force): Officers may review their own BWC recording when they are:
   1. Involved in an incident, for the purposes of completing an investigation and preparing official reports. To help ensure accuracy and consistency, officers should review the BWC recording prior to preparing reports;
   2. Preparing for court. Officers should advise the prosecuting attorney that they reviewed the BWC recording; and
   3. Providing a statement pursuant to an internal investigation or other critical incidents.

   *See* BPD Rule 405, Section 6.2, "Officer Access to Footage Following an Officer Involved Death, Officer Involved Shooting, or Other Use of Deadly Force (Rule 205 and/or Rule 303 Investigations)."

   Officers who need to review video or audio footage from another officer shall make a request via the online Special Notification Form to the Video Evidence Unit describing why they need to review the footage.

   The Commander of the Video Evidence Unit shall approve or deny the request. With approval, the Video Evidence Unit will provide access to the video and audio footage to the requesting officer. If providing another officer's video or audio, the Video Evidence Unit shall notify the District or Unit Commander of the officer whose BWC footage is requested that the BWC footage is being shared.

   Any supervisor within the recording officer's chain of command, and any Bureau Chief, may review the footage consistent with Section 4.2 of BPD Rule 405. A supervisor outside of the chain of command shall only be allowed to review footage with the permission of the Video Evidence Unit Commander.

The Department will give detectives access to all BWC footage related to their assigned cases.

When assigned a case for investigation, the assigned detectives will:

1. Determine the identity of all involved officers.
2. Search evidence.com for any associated BWC media, using applicable search parameters to verify that they have located all relevant files.

The assigned Detective will review all BWC footage within a reasonable time. However, if the Detective determines that the BWC footage is not relevant to the investigation or the investigation is closed, the Detective may, with the approval of their supervisor, choose not to review the BWC footage. The supervisor's approval shall be noted in the case management file.

Detectives should be aware that additional BWC footage may be updated at a later time or date.

Should a detective consider material too sensitive to be accessible for other members of the Department, the detective shall notify his/her supervisor of the sensitive material. The detective's supervisor shall review the video and, if deemed appropriate, send a request via the BWC Special Notification Forms to the Video Evidence Unit to make the data unavailable for a given amount of time.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

BWC recordings and data are kept in a cloud-based storage platform managed by Video Evidence Unit.

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

The Department will retain BWC footage based on categorization, but may retain the footage longer on a case-by-case basis as determined by the Police Commissioner or his/her designee. The footage retention schedule for cloud-based footage access is as follows:

a. Schedule I- Indefinite Retention:
    • Death Investigation
    • Code 303- Lethal/Less Lethal
    • Sexual Assault / Abused Person

b. Schedule II- 7 Year Retention:
    • Use of Force
    • Arrest
    • Felony - No Arrest

c. Schedule III- 3 Year Retention:
    • Misdemeanor - No Arrest
    • Investigate Person
    • Investigate Premise

d. Schedule IV- 180 Day Retention:
    • Significant Event - Public Safety
    • Traffic Stop
    • Encounter/FIO
    • Sick Assist
    • No Report - Dispatch / On Site
    • Test/Training
    • Accidental Recording

If an officer requests access to footage be made available for a time frame longer than the retention schedule allows, a request to extend retention schedule via the BWC Special Notification Form must be sent to the Video Evidence Unit.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

**Public Information Requests:** Video Evidence Unit shall respond to public information requests submitted under G.L. ch 66, § 10, in accordance with all applicable state laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

**Other External Information Requests:** Civil discovery requests are appropriately submitted to the assigned attorney in the Office of the Legal Advisor, and requests for information submitted by a collective bargaining representative under M.G.L. c. 150E are appropriately submitted to Office of Labor Relations. Should an officer receive a civil case subpoena or court order, he or she shall forward the request directly to the Office of the Legal Advisor. If these offices receive other external requests for BWC footage, they shall request necessary and responsive footage from the Video Evidence Unit via the online BWC Special Notification Form.

The Video Evidence Unit shall maintain a log of the request, and assist the requesting office to collect and process the requested footage. The Video Evidence Unit shall provide the requested footage to the requesting office, and complete redactions if required by the requesting office. The requesting office will be responsible for the review, approval, and release of footage to the appropriate person(s) as consistent with applicable law and agreements.

**Media Requests:** All media requests made related to surveillance data from a ShotSpotter will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

**Criminal Defendants:** 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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

Federal, state, and local prosecutors shall make requests for BWC footage directly to the Video Evidence Unit. 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, Video Evidence Unit ("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, 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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Prior to being issued a BWC, officers shall successfully complete BPD Academy training related to this policy as well as the activation, use, categorization, and uploading of data.

All department personnel who may supervise officers wearing BWCs or will require access to review videos shall also attend Department approved training. Detectives will not use the BWC system or evidence.com until they have successfully completed the required training.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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

    Commanding officers or his/her designee will review BWC activity logs and reports to ensure officers remain in compliance with Department policy and training.

    Audit and Review shall conduct periodic checks to ensure Department personnel are using BWCs according to Department policy.

    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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department use of BWCs and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department use BWCs and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix H: Boston Police Department Rule 205**
- **Appendix J: Boston Police Department Rule 303**
- **Appendix S: Boston Police Department Rule 405**

**Department: Boston Police Department**
**Surveillance Technology: Cameras and Video Management Systems**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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 and otherwise assist officials with the provision of municipal services in order to enhance overall municipal efficiency, and assist with the training of department personnel.

   The Boston Police Department's video management systems are governed by the Metro Boston Homeland Security Region's Critical Infrastructure Monitoring System (CIMS) Closed Circuit Television (CCTV) Policy. The BPD Video Management Systems (VMS) Policy is consistent with and builds on the Metro Boston Homeland Security Region ("MBHSR") policy.

   As of August 1, 2022, BPD's Bureau of Administration and Technology (BAT) maintains a network of approximately 1,000 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. The Department currently uses the FLIR Video Management System to view the cameras on the BAT Camera System.[1]

   The Boston Police Department has direct access to 380 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 the Genetec Video Management System to view the cameras on the DoIT/BTD Camera System.

   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

[1] Additional cameras record video at BPD District police stations (in public areas and holding areas) and are separate from and not incorporated on the BAT Camera System.

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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   The Department uses the BAT Camera System and the DoIT/BTD Camera System for official law enforcement purposes or to fulfill Public Records Requests or subpoenas only. Any personal use of either camera system is strictly prohibited.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   Video: live stream and recording ("VMS Video"). The BAT Camera System and the DoIT/BTD Camera System are active twenty-four (24) hours a day, seven (7) days a week ("24/7"). The Department does not monitor the live stream of the BAT Camera System or DoIT/BAT Camera System 24/7.

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

   The cameras do not have facial recognition capabilities. The cameras do not have any audio capabilities.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Boston Police Department Personnel: All BPD personnel who require or request access to view the live feed of the BAT Camera System are approved through the BPD Bureau of Administration and Technology (BAT). The BAT/Video Evidence Unit (VEU) will create user groups that will administratively allow access to certain cameras within the system for department employees that have been granted permission to use the system. Limited users have access to all cameras on the BAT Camera System. *See also* BPD Rule 322 (Department Property).

   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.

No commercial or private individuals have access to the BAT Camera System.

The City of Boston and BTD control user access to the DoIT/BTD Camera System. The City of Boston/BTD has provided a limited number of users within the Department access to the DoIT/BTD Camera System.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

The network servers shall be maintained in a secure environment. Recordings shall be stored in such a manner that the particular images can be identified by camera location and by the date and time recorded.

Anyone who engages in an impermissible use of the camera system(s) may be subject to criminal prosecution, civil liability, and/or administrative sanctions up to and including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

Violations of this policy occur when an individual utilizes the camera system(s) for purposes including, but not limited to:

- Invasion of Privacy. Except pursuant to a court order, it is a violation of BPD Policy to observe, or record footage of, locations except those that are in public view from a vantage point that is accessible to the general public and where there is no reasonable expectation of privacy. Areas in which there is a reasonable expectation of privacy include the interior of private premises such as a home.

- Harassment/Intimidation. It is a violation of BPD Policy to use the camera system(s) to harass and/or intimidate any individual or group.

- Use / Observation Based on a Protected Characteristic. It is a violation of BPD Policy to use the camera system(s) to observe individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classification protected by law.

- Personal Use. It is a violation of BPD Policy to use the camera system(s) for any personal purpose.

- First Amendment Rights. It is a violation of BPD Policy to use the camera system(s) for the purpose of infringing upon First Amendment rights.

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received,

disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

VMS Video -- that is, video recordings from the BAT Camera System and the DoIT/BTD Camera System -- shall only be downloaded and copied by members of the Boston Police Department's Video Evidence Unit. BPD requests for archived VMS video shall only be accepted via an internal request link that can be found on the BPD intranet. That request will be logged and processed once it is received. The Video Evidence Unit is the keeper of records for all requests made via the Department website as well as subpoenas.

Recorded video is retained for 30 days unless a request has been made to preserve the footage from a BPD employee, an outside law enforcement agency, a prosecutor or criminal defendant, or from internal personnel fulfilling a Public Records Request or subpoena.

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

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.

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data from Department cameras and Video Management systems are handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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.

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 CIMS/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 MSHSR 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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

The Video Evidence Unit provides training for users.

In anticipation of promotion, Supervisors and Detectives receive training at the Academy to learn the operations of both the FLIR and GENETEC systems as end users. Class instruction shows user how to access the systems and search for archived video. Users are informed that there is an auditing system built into both systems. Users are also shown how to request video via internal BPD links.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

The Police Commissioner or his/her designee will designate the number of System Administrators allowed to grant and oversee access to the BAT Camera System. System Administrators are designated based upon their subject matter expertise to the MBHSR CIMS program and do not hold operational functions that would create a conflict of interest. System Administrators have the ability to create groups and assign permissions

based upon job function or assignment. Permissions are determined by the System Administrator and include the capabilities to view, rewind, download, or restrict camera footage.

All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department.
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).

The CIMS project is overseen and managed by the MBHSR 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 amount of instances where real-time camera access was granted by a jurisdiction to a requesting agency.

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department use of cameras and video technology will be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department use of cameras and video technology will be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix Y: Boston Police Department Special Order 22-8 (BPD Video Management Systems Policy)**
- **Appendix MM: Metro Boston Homeland Security Region's Critical Infrastructure Monitoring System (CIMS) Closed Circuit Television (CCTV) Policy**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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 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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

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

   Generally, BPD investigators must first obtain a search warrant allowing for the use of the device. The search warrant is obtained with the aid of a State or Federal prosecutor with proper jurisdiction. The BPD investigator and prosecutor must make an application to a judge for a search warrant. The search warrant can only be issued by a judge. The application must be made under oath. For a judge to grant a search warrant, the judge must find there is probable cause to believe a person has committed, is committing, or is about to commit a crime, and the use of a cell-site simulator will be relevant to the investigation. BPD personnel must use the cell-site simulator in accordance with the terms of the warrant. *See* BPD Rule 334 (Search Warrant Application and Execution).

   A cell-site simulator may be used without a search warrant if exigent circumstances exist. In those instances, an BPD investigator must have probable cause to believe: (1) an emergency exists as result of the criminal conduct; (2) there is an immediate urgent need for assistance due to an imminent danger of serious bodily injury or death to any person; and (3) the effort to locate a suspect is being undertaken with the primary concern of preventing serious injury or death and is not primarily motivated by an intent to arrest

and seize evidence. The possibility of flight of a suspect does not on its own constitute exigent circumstances.

When exigent circumstances exist, the BPD investigator or Supervisor must first document the nature of the emergency and collect all relevant information pertaining to the incident. The BPD Investigator or Supervisor will then contact the Commander of the Special Investigations Unit (SIU) or their designee and relay all pertinent information relative to the incident. In conjunction with BIS Command, a decision will be made to determine if the facts of the incident meet the exigent circumstance standard and whether a cell-site simulator will be used.

While the cell-site simulator may be used without a search warrant for up to forty-eight (48) hours in exigent circumstances, a search warrant will be obtained for any exigent circumstances which exceed the forty-eight (48) hours to continue the use of a cell site simulator.

BPD personnel involved in the use of the cell-site simulator may only utilize the technology to execute their lawful duties, which relate only to official business of the BPD and for legitimate law enforcement purposes.

Only members of the SIU can access and operate the cell-site simulator and associated equipment.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

Cell-site simulators acquire limited information from cellular devices.[1]

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 and will not be used to collect the contents of any communication or any data contained on the device itself. The cell-site simulator cannot and will not be used to capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an account

[1] 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.

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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   The cell-site simulator may only be used by BPD personnel for legitimate law enforcement purposes.

   Only members of the SIU can access and operate the cell-site simulator. *See also* BPD Rule 322 (Department Property). The cell-site simulator will only be used after SIU has received all of the proper information and upon receiving approval from BIS Command.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   The cell-site simulator is securely stored within BPD facilities when not in use and in a location secured from the public. Additionally, a SIU Supervisor must periodically inspect the cell-site simulator. Access to the cell-site simulator is limited to SIU personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to BPD cell-site simulator technology is removed when access is no longer necessary for BPD personnel to fulfill their duties (*e.g.*, when personnel are transferred from SIU to another unit).

   Authorized users of the cell-site simulator software are authenticated by a username and password. Access to the software is critically limited to SIU personnel who have received training in the use of the technology. Cell-site simulator software can only be accessed by SIU on a laptop that operates on a closed, stand-alone network. The network utilizes industry best standards and practices to prevent external penetration and unauthorized usage.

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The cell-site simulator will only be used for the time period authorized by the search warrant obtained by the SIU or BPD investigator, or while the exigency or emergency persists.

A warrant is required for the continued use of the cell-site simulator in any exigent event that exceeds forty-eight (48) hours in duration.

Upon expiration of the court order or exigent circumstances, use of the cell-site simulator in connection to that particular investigation is terminated, and the physical device is returned to SIU.

The BPD's deletion of the data or information received by the cell-site simulator or associated software will include the following practices:

1. When the equipment is used to locate a cellular device with a known unique-identifying number, all data should be deleted once the device is located and secured, or no later than 24 hours after the device is located.
2. When the equipment is used to identify a cellular device with an unknown unique-identifying number, all data must be deleted as soon as the target cellular device is identified, or no later than 30 days from its collection.
3. Prior to deploying equipment for a new mission, the operator must verify that the equipment has been cleared of any previous operational data.

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

   All media requests made related to surveillance data from a ShotSpotter will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

   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.

8. **Information and Data-Sharing:**
   a. **How can other City or non-City entities access or use the Surveillance Data?**
   b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
   c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

   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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

SIU personnel are trained in the use and operation of the cell-site simulator and associated software by the vendor providing the technology. BPD personnel must use the cell-site simulator in compliance with BPD policies and training.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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. A cell-site simulator will not be used without proper approvals, even in exigent circumstances.

Supervisors of personnel utilizing the cell-site simulator are responsible for security and proper utilization of the technology.

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 the Internal Affairs Division (IAD).

The SIU will ensure all information related to the Department's use of the cell-site simulator required under Chapter 16-63.5 of the City of Boston Municipal Code (Ordinance on Surveillance Oversight and Information Sharing) is provided to the Office of the Police Commissioner on an annual basis.

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department use of the cell-site simulator and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department use of the cell-site simulator and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix Q: Boston Police Department Rule 334 (Search Warrant Application and Execution)**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The Bureau of Investigative Services (BIS), Special Investigations Unit (SIU) and Drug Control Unit (DCU), the Bureau of Intelligence and Analysis (BIA), Boston Regional Intelligence Center (BRIC), and the Bureau of Field Services (BFS), Youth Violence Strike Force (YVSF) 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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Use of covert audio and video devices shall be limited to only BPD personnel authorized by the Department to deploy the devices in the course and scope of their employment to support the investigatory functions and/or community caretaking responsibilities of the Department.

   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. Mora*, 485 Mass. 360 (2020); *see also* BPD Rule 334 (Search Warrant Application and Execution).

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Covert audio and video devices shall be stored in a secure location, and all access and use of the devices shall be documented in an investigative file. Any recorded audio or video

data collected by the devices shall be stored in the physical case file and/or stored within a BPD-approved electronic case/content management system (*i.e.*, "Detective Case Management"). Access to audio and video data (real-time or recorded) captured by covert devices shall be limited to authorized BPD personnel for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

   All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

   Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at:

https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data from a Department UAS will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

    Training on the operation of covert devices is provided by the vendors.

    Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

    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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department covert cameras shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to *Commonwealth v. Mora*, 485 Mass. 360 (2020), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department covert cameras shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to *Commonwealth v. Mora*, 485 Mass. 360 (2020), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

**<u>Department</u>: Boston Police Department**
**<u>Surveillance Technology</u>: Covert Audio and Video Devices**

**Attachment:**

- **Boston Police Department Rule 334 (Search Warrant Application and Execution)**

**Department: Boston Police Department**
**Surveillance Technology: Crime Laboratory Unit**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The Crime Laboratory Unit utilizes devices, hardware, and software to provide services including:[1]

   - 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
     - Paint and glass analysis

   The Crime Laboratory Unit does not utilize any "mobile DNA capture technology."

   CODIS is a computer database that can be used to generate investigative leads through the comparison of DNA profiles.

   The CODIS database 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.

   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.

[1] The Crime Lab 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" and subject to the use, access, data protection, retention, public access, info sharing, training, oversight, legal authority, and child rights information therein.

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 profiles meet certain criteria.

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

Casework samples are analyzed using a minimum of the 13 core STR loci according to procedures described in the DNA Lab Manual. The 13 core CODIS loci are: D3S1358, vWA, D16S539, CSF1PO, TPOX, D8S1179, D21S11, D18S51, TH01, FGA, D5S818, D13S317, and D7S820.

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. |

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.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   The CODIS database 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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Members of the DNA Section have been assigned specific roles in the CODIS program. The roles are described below:

   **CODIS Administrator:** The CODIS Administrator role will be filled by a qualified individual appointed by the DNA Section supervisor or Technical Leader. The CODIS Administrator shall be an employee of the laboratory, and must be, or have been, a qualified DNA analyst. (Have six months of documented forensic human-DNA laboratory experience, performed analysis on a range of samples routinely encountered in forensic casework, have documented mixture interpretation training, and completed a competency test). The CODIS Administrator will manage the overall CODIS program. This will include responsibility for administering the laboratory's local CODIS network, scheduling and documenting the CODIS computer training of casework analysts, assuring that the security of data stored in CODIS is in accordance with state and/or federal law and the National DNA Index System ("NDIS") operational procedure, assuring that the quality of data stored in CODIS is in accordance with state and/or federal law and NDIS operational procedures. The CODIS Administrator is responsible for ensuring the security and restricted access of CODIS, handling any computer or network- related issues, management and assignment of computer passwords and privileges. Additional duties include data entry, data upload and search, and match interpretation, management, and reporting. The CODIS Administrator will provide documentation of completion of the FBI auditor training, or will complete such training within one year of appointment. The CODIS Administrator will provide documentation of completion of the FBI CODIS software training, or will complete such training within six months of appointment.

   The CODIS Administrator is authorized to terminate an analyst's, or the laboratory's, participation in CODIS until the reliability and security of the computer data can be assured, if an issue with the data is identified.

   **Alternate CODIS Administrator:** CODIS Administrator privileges will be given to a second qualified or previously qualified DNA analyst from the laboratory to serve as Alternate CODIS Administrator. The Alternate CODIS Administrator will serve as the

CODIS Administrator in the absence of the primary CODIS Administrator. The Alternate CODIS Administrator is subject to the same education and training requirements as the CODIS Administrator, listed above.

Both the CODIS Administrator and the Alternate CODIS Administrator will have an elevated user account.

**CODIS Analyst:** All authorized casework analysts in the DNA Section may generate casework DNA profiles for entry into CODIS. Authorized analysts may also enter DNA profiles into CODIS, verify data entry in a Candidate Match, and determine if Candidate Matches should be confirmed.

All CODIS Users (Administrators and Analysts) are subject to the requirements of the most current NDIS Procedures Manual.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   The CODIS server is located in the Examination Room within the Crime Laboratory. CODIS workstations are located in Office rooms S259 and S263. Electronic access to the CODIS computer and its information is limited to the members of the DNA Section, or to members of the Informational Systems Group (ISG) Department only in the presence of a member of the DNA Section with CODIS access. Each member of the DNA Section will have a unique user ID and password which are required for access to the CODIS computer. Additionally, the CODIS Administrator and Alternate CODIS Administrator will have elevated user access to CODIS.

   To further ensure the integrity of the CODIS computer and its contents, the system is backed up after hours by backup Tape Monday through Friday. It is recommended that a new tape is inserted every week and rotated each week of the month (a minimum of 4 total tapes). The active tape will be in the server. The other, inactive tapes for the month will be stored in a key-locked safe within the monitored and limited access Crime Laboratory Unit.

   Additionally, ideally done in the first week of every month, a monthly backup is performed, and sent off-site to a secure location at BPD Records and Archives. BPD Records and Archives is a limited access facility which is secured and monitored. The monthly backup media are stored in a key-locked safe at BPD Records and Archives. Several tapes and/or other media will be kept, and rotated through to serve as the off-site monthly backup.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**

**c. What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

A casework DNA profile will be deleted (expunged) from the database
a. If the DNA profile is found to be consistent with:
a. The victim
b. An elimination standard (e.g. husband, consensual partner)
b. If information is obtained to indicate that the DNA profile is ineligible for CODIS entry. (e.g. was obtained from an evidence item collected from the suspect's person, or in the possession of the suspect when collected by law enforcement.)

**7. Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

CODIS is not a public system.

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data from a ShotSpotter will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

**8. Information and Data-Sharing:**
**a. How can other City or non-City entities access or use the Surveillance Data?**
**b. How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
**c. What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

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 autoscheduled 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.

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

All employees in the Crime Lab must complete technical/administrative training programs before assuming responsibilities. Technical staff undergo competency testing before assuming responsibilities. Crime Lab personnel undergo annual proficiency tests in each discipline he/she is authorized to perform testing.

Additional training materials are available in the CODIS Training Manual or the CODIS Web site.

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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

    There were no reported non-conformances in the last full assessment (2021). There were no reported non-conformances in the last surveillance audit (2022).

    **Internal Audits:** Management reviews are conducted annually in the Crime Laboratory 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 Crime Laboratory Unit. A DNA QAS audit is conducted internally every other year.

    **External Audits:** Full assessment every four years in the accredited units. Surveillance audits every year, with the exception of full assessment years. Alternate internal/external QAS audits every calendar year.

    **CODIS:** A CODIS Laboratory must have properly trained personnel, a well-managed facility, and validated procedures for sample collection and subsequent DNA analysis. The FBI is responsible for ensuring that laboratories that participate in CODIS meet national standards for quality assurance and quality control. To ensure that the Boston Police Crime Laboratory meets quality standards, the DNA Section of the Crime Laboratory was first inspected by the National Forensic Science Technology Center (NFSTC) in August of 1998, and found to be in compliance with the FBI's Quality Assurance Standards (QAS). The DNA Section has maintained ongoing compliance with the QAS since August, 1998 and accreditation since June, 2002.

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    The Crime Lab utilizes devices, hardware, and software, including, but not limited to, the CODIS database, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The Crime Lab utilizes devices, hardware, and software, including, but not limited to, the CODIS database, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation:

- **Appendix HH: Boston Police Department Crime Laboratory CODIS Manual**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

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.

As set out in the Preamble to G.L. ch. 272, § 99 (Interception of wire and oral communications):

> The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as it exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living.
>
> The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminating it. Normal investigative procedures are not effective in the investigation of illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities.
>
> The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

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.

Pursuant to 18 U.S.C. § 2518:

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:
   (a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;
   (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;
   (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
   (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe

that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

> (4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—
>
> (a) the identity of the person, if known, whose communications are to be intercepted;
>
> (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
>
> (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
>
> (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
>
> (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

*Accord* G.L. ch. 272, § 99 (requirements for application for a search warrant and procedure required to intercept wire and oral communications under state law).

**3. Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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.

**4. Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

The core LINCOLN System is built on server hardware and client/server software that is run on a local area network in the wireroom. The client workstations on the LAN run a network installation of PenLink software.

One Administrator manages the System and assigns access (permissions and roles) to the System. Access is determined on a case-specific basis and only available to the use for the duration of the investigation. All users must have passwords to access the System. Users may access the System for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   The System Administrator can monitor all user activities.
   The System is in a locked, secure room and only available to the user for the duration of the investigation. Users cannot delete, print, copy or share any data unless they have full access rights, which only the Administrator has.

   All data collected is stored in a secure server and only the Administrator has access. The System has a full audit function and embedded security features to prevent tampering. The location of the security features is only known to the vendors' engineers.

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

   All data is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

   Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

   Likewise, data collected pursuant to federal authorization is maintained in accordance with federal records retention schedules.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations.

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

   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.

8. **Information and Data-Sharing:**
   a. **How can other City or non-City entities access or use the Surveillance Data?**
   b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
   c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

   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).

9. **Training:**
   a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
   b. **What are the training materials?**

Initial training on the System is conducted by the vendor. Subsequent user training is conducted by the Administrator.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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

    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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    The use of the System and collection and maintenance of data is in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws, including, but not limited to 18 U.S.C. § 2518 and G.L. ch. 272, § 99, and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The use of the System and collection and maintenance of data is in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws, including, but not limited to 18 U.S.C. § 2518 and G.L. ch. 272, § 99, and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

**Attachments:**

- **18 U.S.C. § 2518**
- **G.L. ch. 272, § 99**

**<u>Department</u>: Boston Police Department**
**<u>Surveillance Technology</u>: Electronic Intercept & Analysis System ("Wire Room")**

- **Boston Police Department Rule 334 (Search Warrant Application and Execution)**

**Department: Boston Police Department**
**Surveillance Technology: Firearms Analysis Unit**

1. **Purpose: What is the purpose of this Surveillance Technology?**

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

- Crime scene processing including evidence documentation and collection[1]
- 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)[2] 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,

[1] 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" and subject to the use, access, data protection, retention, public access, info sharing, training, oversight, legal authority, and child rights information therein.

[2] 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.

and more. These reports provide a snapshot view of potential firearm trafficking indicators

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   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.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Information is made available electronically thru a secure https website.

   eTrace access is achieved by obtaining a valid User Id. and password from ATF and authenticated using the eTrace site on the internet. Each participating agency also enters into a Memorandum of Understanding (MOU) with ATF. The MOU is intended to formalize a partnership between the participating agencies with regard to policy and procedures relative to the access and utilization of eTrace services. Successful access allows users the ability to enter new traces, view existing traces, and run reports on traces for which they are authorized.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   In accordance with applicable appropriations laws, eTrace users can only access trace data that originated from their agency. In addition, the eTrace system includes the standard HTTP Level banner on the bottom of each web page which reads, "You have entered an Official United States Government System, which may be used only for authorized purposes. The government may monitor and audit usage of this system, and

all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Section 1001 and 1030."

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The data is retained pursuant to rules and schedules set by the National Archives and Records Administration (NARA).

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

eTrace is not a public system. eTrace is only available to approved Federal, State and local law enforcement agencies.

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

eTrace is available only to official law enforcement agencies (local, state, federal and international) that have entered into a Memorandum of Understanding (MOU) with ATF acknowledging procedures, conditions, and terms of use.

9. **Training:**
   a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
   b. **What are the training materials?**

All employees in the FAU must complete technical/administrative training programs before assuming responsibilities. Technical staff undergo competency testing before assuming responsibilities. Firearms Analysis Unit analysts also undergo annual proficiency tests in each discipline he/she is authorized to perform testing.

eTrace is a user-friendly web-based application for use by official law enforcement agencies only. An eTrace User's Guide is available online.

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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

There were no reported non-conformances in the last full assessment (2021). There were no reported non-conformances in the last surveillance audit (2022).

**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.

The MOU with each agency will designate a primary and alternate point of contact within each agency. The agency point of contact will be charged with ensuring adherence to the MOU between ATF and the agency users. The MOU will require the designated agency point of contact to identify individuals from their respective agency who will require system access, to periodically validate the list of users and to notify the National Tracing Center immediately in the event that it becomes necessary to revoke or suspend a user's account.

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    The FAU utilizes devices, hardware, and software, including, but not limited to, the eTrace database, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The FAU utilizes devices, hardware, and software, including, but not limited to, the eTrace database, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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 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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   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.

   Data extraction/examination forensic tools and software and associated data shall not be used for personal purposes. The equipment shall not be used for illegal purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   The data collected by extraction/examination forensic tools and software shall be stored in the physical case file and/or stored within the Department's electronic case management system. *See* also BPD Rule 322 (Department Property).

   Access to the data generated through the use of extraction/examination forensic tools and software shall be limited to investigators to utilize the data in the course and scope of law enforcement and investigatory purposes.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   The Department utilizes physical access controls, application permission controls, and other technological, administrative, procedural, operational, and personnel security measures to protect data collected by extraction/examination forensic tools and software from unauthorized access, destruction, use, modification, or disclosure.

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, only as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

    All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

    Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

    BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

    Absent a court order, the public shall not have direct access to data collected by data extraction/examination forensic tools and software.

    All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

    All media requests made related to surveillance data from Department forensic exam hardware/software will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

    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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

    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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

    Electronic Crimes Investigators assigned to the Boston Police Department Forensic Group who utilize forensic examination hardware receive multiple trainings, including, but not limited to, training from the United States Secret Service in the recovery of digital evidence using forensic techniques, and analysis of digital evidence. Investigators are certified forensic computer and cellphone examiners.

    Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

    The Department will ensure compliance with all applicable laws. 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.

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department forensic exam hardware and software shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department forensic exam hardware and software shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including, but not limited to, Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix Q: BPD Rule 334 (Search Warrant Application and Execution)**

**Department: Boston Police Department**
**Surveillance Technology: Gang Assessment Database**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The purpose for the existence of the Gang Assessment Database is to:

   1. Provide law enforcement a consistent citywide framework for identifying individuals and groups that associate as a "gang" and thus are likely to engage in or perpetrate criminal activity for the furtherance of the criminal organization, which may include targeted and/or retaliatory violence; and
   2. Assist in the investigation of gang related criminal activity in the City of Boston.

   The database 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.

   The Department has partnered with the Safe and Successful Youth Initiative (SSYI) to provide services as a pathway out of gang involvement. The SSYI Database is an electronic case management system that includes individual-level data on SSYI clients. Individuals referred by the BPD's Youth Violence Strike Force and by other SSYI Law Enforcement partner agencies (Massachusetts Department of Youth Services, Probation Service, Department of Correction, Suffolk County House of Correction, District Attorney's Office) to the SSYI Program Coordinator/Law Enforcement Lead (civilian), are considered for participation in the program. Through community-based partnerships, suitable individuals in the database with whom the Youth Violence Strike Force (YVSF) makes contact are referred to social services and offered a variety of opportunities.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   **Use of the Gang Assessment Database:** BPD Rule 335 (Gang Assessment Database) with revisions implemented by Special Order 21-27, dated June 8, 2021, and the Boston Regional Intelligence Center (BRIC) Privacy, Civil Rights, and Civil Liberties Protection Policy (2021), govern the Gang Assessment Database.

   The information in the Database is considered Law Enforcement Sensitive and is thereby For Official Use Only. It is to be used within the law enforcement community to assist in the prevention, investigation and resolution of criminal activity. The release of this

information, to the public or other personnel who do not have a valid "need-to-know," without the prior approval of the commanding officer of the BRIC 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, improperly disclose witness identity information and thereby compromise officer safety as well as that of the public.

**Submission to the Gang Assessment Database:** Authorized Users will be able to submit an individual for consideration for admission into the Gang Assessment Database. All submissions for verification shall include documentation to support the individual's entry into the Gang Assessment Database using the Point-Based Verification System. Submissions can be made to the Commander of the BRIC or their designee or the Commander of the Youth Violence Strike Force or their designee.

All submissions for verification will be manually reviewed by a BRIC civilian analyst and supervisor to determine compliance with BPD Rule 335 prior to entry into the database. If the individual is verified as a gang associate, the supporting documentation shall be maintained by the BRIC in the Gang Assessment Database.

No individual will be considered for addition to the Gang Assessment Database on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

**Participation in the SSYI Program:** Individuals referred by the BPD's Youth Violence Strike Force and by other SSYI Law Enforcement partner agencies (Massachusetts Department of Youth Services, Probation Service, Department of Correction, Suffolk County House of Correction, District Attorney's Office) to the SSYI Program Coordinator/Law Enforcement Lead (civilian), are considered for participation in the program. The criterion-based vetting process for individuals identified as eligible after having satisfied the following SSYI Eligibility Criteria, including:

An Eligible Individual is an individual who is 17 to 24 (inclusive) years old who

a. Is known to law enforcement as meeting at least one of the following criteria:
    i. Repeatedly engages in crimes against persons;
    ii. Repeatedly engages in weapons violence;
    iii. Is in a leadership role in a gang;
    iv. Is substantially involved in gang activity or street violence; or
    v. Significantly facilitates gang activity or street violence; and
b. Currently resides in the Grantee's community, spends a significant amount of time in the community, or is expected to be released into the community.

Once eligibility is verified by the SSYI Data Analyst, the eligible individual is entered into the SSYI Database by the BPD's SSYI Program Coordinator/Law Enforcement

Lead, who reviews and updates the eligibility status of each eligible individual on an ongoing basis. Any individual added or removed from the service cohort is done by the SSYI Program Coordinator/Law Enforcement Lead. The Department does not have any further access to the SSYI database.

Following successful outreach by the SSYI case managers from the Lead Community-Based Agency, the Boston Public Health Commission (BPHC), individuals identified as SSYI eligible complete intake, enrollment, and assessment tasks prior to being offered intervention services. The SSYI case managers document all program and participant services and activities in the database. Access to this information is limited to the case management team at BPHC and is not available to BPD.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

The Gang Assessment Database is an electronic database maintained by the BRIC that includes Gang Associates and Gangs in accordance with BPD Rule 335 (Gang Assessment Database).

The BRIC will maintain copies of supporting documentation for all criteria used to verify an individual. The BRIC will analyze the validity of the supporting documentation for each individual criteria used to verify an associate and maintain the discretion to decline to use the information towards any criterion. The BRIC will maintain the discretion to decline to enter individuals into the database who meet the 10 point criteria but are determined to not be engaged in gang-related criminal activity.

The SSYI Database is an electronic case management system that includes individual-level data with personal identifiable information on SSYI clients.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

The Department will provide access to the Gang Assessment Database to all personnel defined as authorized users in Section 4.11 of BPD Rule 335.[1] All authorized users must complete a User Agreement before gaining access. Authorized users must have a legitimate law enforcement purpose for accessing the Gang Assessment Database. The Boston Regional Intelligence Center (BRIC) will serve as the administrator of the database and ensure that users have adequate access.

Authorized Users will have the following access permissions:

- READ all Gang Assessment Database entries within the system

[1] "Authorized User" is defined as: All sworn Boston Police Officers and other individuals designated by the Commander of the Bureau of Intelligence and Analysis or his/her designee, in collaboration with the Commander of the Youth Violence Strike Force or his/her designee, shall be granted access to the Gang Assessment Database in accordance with BPD Rule 335.

- SEARCH all Gang Assessment Database entries within the system

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 database shall be logged and the reason and recipient noted.

Access to the SSYI database is limited to the SSYI Program Coordinator/Law Enforcement Lead (civilian) and the SSYI Data Analyst(s) to update the eligibility status of each eligible individual on an ongoing basis. SSYI case managers document all program and participant services and activities in the database, and access to this information is limited to the case management team and is not available to BPD.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

The Police Department is audited every three (3) years by FBI CJIS to ensure that we, as a Department, adhere to the standards defined in the Criminal Justice Information Security Policy. The most recent audit was conducted in July 2021. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Boards decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST).

The CJIS Security Policy defines standards for everything from physical security, network security, log file retention, encryption requirements (FIPS 140-2) to security awareness training. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage and destruction of Data. This Policy applies to every individual, contractor, with access to or who maintain and support information services.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The Commander of the BIA or his/her designee, in collaboration with the Commander of the Youth Violence Strike Force or his/her designee, shall be responsible for ensuring that files are maintained in accordance with the goals and objectives set forth in BPD Rule 335.

Entries in the Gang Assessment Database shall be reviewed at least once every five years to determine if the individual remains active based on the definitions provided in BPD Rule 335, Sections 4 and 5. When an individual no longer meets the criteria for Active Status, they will be purged from the system by a BRIC analyst. This five-year period is consistent with 28 CFR Part 23 (Criminal Intelligence Systems Operating Policies) and the retention of criminal intelligence information.

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

All data contained in the Gang Assessment Database is considered Law Enforcement Sensitive. Members of the public may seek to know the existence of and to review the information about him or her that has been gathered and retained by the BRIC and may obtain a copy of the information and to challenge the accuracy or completeness of the information (correction) pursuant to the BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy (2021), Section K (Redress).

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at:
https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All court ordered, defense requested, or public record requested production of information contained in the Gang Assessment Database should be directed to the Boston Police Department's Office of the Legal Advisor.

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

All mutual aid or assistance requests by 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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

All Authorized Users of the Gang Assessment Database are trained on its operation and BPD Rule 335 prior to their access being granted. This includes training for new recruits in the BPD Police Academy and refresher training during Detective and Sergeants courses. Additional training is provided periodically as the technology is updated or rule changes are implemented. Training is provided by BRIC subject matter experts, including analysts and supervisors.

All BRIC analysts receive at least 40 hours of training per year. New analysts are extensively trained by their supervisors and peers on all policies and procedures relevant to their roles and responsibilities. Ongoing refresher training is provided to all personnel on a periodic basis as needed.

Analysts are trained in accordance with the Analyst Professional Development Road Map, Version 2.0, produced in 2019 by the U.S. Department of Justice, Bureau of Justice Assistance, the Global Information Sharing Initiative, and the Department of Homeland Security.

Additionally, all BRIC personnel are trained at least annually on the BRIC Privacy Policy and 28 C.F.R. Part 23 (Criminal Intelligence Systems Operating Policies), as well as all other relevant BRIC policies and standard operating procedures.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

BRIC will report by January 31st of each year to the Police Commissioner on the total number of individuals added to and purged from the database in the previous calendar year. These totals will then be released to the public.

The BRIC will be open with the public in regard to information and intelligence collection practices. The Center's Privacy Policy will be provided to the public for review, made available upon request, and posted to http://www.bpdnews.com and the National Fusion Center Association Web site (http://new.nfcausa.org/).

The BRIC's Privacy Officer, on behalf of the Privacy Committee, will be 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 center.

The BRIC will maintain an audit trail of accessed information from the Gang Assessment Database. 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.

The BRIC will adopt and implement procedures to evaluate the compliance of users with the Privacy Policy and with applicable law, to include a review of logging access to BRIC information systems and periodic auditing of user compliance. These audits will be conducted at least annually, and a record of the audits will be maintained by the Privacy Officer on behalf of the Privacy Committee.

If an Authorized User is found to be in noncompliance with the provisions of the Privacy Policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC may:

- Suspend or discontinue access to information by the center personnel, the participating agency, or the Authorized User.
- Apply administrative and/or legal actions or sanctions as consistent with Department rules and regulations or applicable law.
- If the Authorized User is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

Additional details regarding accountability and enforcement are available in the BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy (2021), Section N (Accountability and Enforcement).

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).

**11. Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

The Gang Assessment Database are used and maintained in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The Gang Assessment Database are used and maintained in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

    The BPD/BRIC is committed to identifying juveniles in the Gang Assessment Database in order to connect them with services. The BPD/BRIC has partnered with Boston's SSYI to provide services as a pathway out of gang involvement.

    The BRIC will notify the SSYI Lead Community-Based Agency, the Boston Public Health Commission (BPHC) and the Director of the Mayor's Office of Public Safety of all juveniles added to the Gang Assessment Database to facilitate connecting juveniles with appropriate services. Provided, however, that SSYI will not be notified if doing so would compromise an ongoing investigation.

    The BRIC will consider the input of SSYI program personnel when determining if a juvenile meets the criteria for exclusion/removal from the Gang Assessment Database.

    It is the ultimate goal of the Boston Police Department to eventually purge all juveniles from the gang database and stop the cycle of violence in the City of Boston.

## Supporting Documentation:

- **Appendix R: Boston Police Department Rule 335 (Gang Assessment Database)**
- **Appendix Z: Boston Regional Intelligence Center Privacy, Civil Rights, and Civil Liberties Protection Policy (2021)**

**Department: Boston Police Department**
**Surveillance Technology: GPS Tracking Units**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Use of GPS trackers shall be limited to only BPD personnel authorized by BPD to deploy the devices in the course and scope of their employment to support the investigatory functions and/or community caretaking responsibilities of the Department. 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).

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   GPS trackers shall 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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   GPS trackers shall be stored in a secure location, and all access and use of the trackers shall be documented in an investigative file.

   The data collected by GPS trackers shall be stored in the physical case file and/or stored within an BPD-approved electronic case/content management system (*i.e.*, "Detective Case Management"). Access to GPS tracking data shall be limited to authorized BPD personnel for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   GPS tracker data is accessible via secure and encrypted web-based application. It is only accessible by authorized BPD personnel who have a username and password.

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**

**c. What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

**7. Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data from a GPS will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

**8. Information and Data-Sharing:**

**a. How can other City or non-City entities access or use the Surveillance Data?**
**b. How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
**c. What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

No outside agencies (City or non-City entities) have direct access to BPD'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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Training on the operation of BPD GPS tracking Units is provided by the vendor.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

All Boston Police Department GPS tracking units shall be deployed, and all data shall be collected, maintained, and utilized, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to, *Commonwealth v. Connolly*, 454 Mass. 808 (2009), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders

GPS tracking 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.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department GPS tracking units shall be deployed, and all data shall be collected, maintained, and utilized, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, but not limited to, *Commonwealth v. Connolly*, 454 Mass. 808 (2009), all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to, Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation:

- **Appendix Q: Boston Police Department Rule 334 (Search Warrant Application and Execution)**

**Department: Boston Police Department**
**Surveillance Technology: Gunshot Detection Technology - ShotSpotter**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   Implemented by the Boston Police Department in 2007, 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. 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 people in possession of guns.

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

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   ShotSpotter uses an array of acoustic sensors that are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately locate gunshots using triangulation. 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.

   Acoustic experts, who are located and staffed in ShotSpotter's 24×7 Incident Review Center, ensure and confirm that the events are indeed gunfire. They can append the alert with other critical intelligence such as whether a fully automatic weapon was fired or whether there are multiple shooters. This entire process takes less than 60 seconds from the time of the shooting to the digital alert popping onto a screen of a computer in the 911 Call Center or on a patrol officer's smartphone or mobile laptop.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   The acoustic sensors capture audio recordings of gunshots or suspected gunshots.

   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 has the gunfire and 1 second of audio prior to and after the gunfire to establish an ambient noise level. Audio snippets are typically only a few seconds long unless there is a gun battle.

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
- 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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Authorized BPD personnel have a ShotSpotter Respond user account. The user can be alerted to real-time notification of gunfire incidents and receive the above-listed data and link to the audio recording from ShotSpotter via email and/or iPhone App. The user can also log into the ShotSpotter Respond web-based portal and access incident information. Authorized BPD personnel may access the portal for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

A limited number of BPD personnel have access to the web-based ShotSpotter Insight portal. ShotSpotter Insight enables customers to explore details about prior gunshot incidents in their ShotSpotter coverage area and use the data for investigation and analysis. Crime analysts, investigators, and command staff can view, filter, sort, report, and transform historical gunshot data into meaningful insights, ultimately informing strategies for reducing gun violence.

Insight enables users to find and identify the incidents using an extensive array of filters for date, time, location, keywords, single vs. multiple gunshots, patrol areas, as well as shapes drawn on the map. The shape filters narrow a search for shooting incidents within a radius of a known address, across several blocks, or look for and monitor activity on both sides of a jurisdictional border. Saved reports retain common filter settings for quick retrieval (*e.g.*, "District 4 Gunfire - Last 28 days").

Insight shows how a shooting event unfolded by watching a shot-by-shot animation that details the location and sequence of each shot. The software also highlights other nearby

incidents that may be potentially related based on its relative distance and time of occurrence. Insight comes with a set of reports that make it easy to share incident data throughout an agency:

• The Investigative Lead Summary report give details of a shooting incident including audio, location, sequence, and timing of each shot fired.
• The Multi-Incident report provides a summary of shooting incidents broken out by single, multiple, and probable gunshot incidents as well as any non-gunfire incidents if they were included in the search. The summary is followed by details for each incident including the date, time, location, number of rounds, CAD ID, Respond ID, and other details.

If the ShotSpotter system misses a gunfire incident, police may contact ShotSpotter to see if there is any audio or location evidence. In this case, only authorized ShotSpotter personnel with proper credentials – and no user from the Boston Police Department – can access sensor audio to search. Their search is limited to the 30- hour sensor storage timeframe. The agency must provide evidence of a shooting in order for ShotSpotter personnel to initiate access to a sensor such as a victim, witness or shell casings. Searching is done visually first, not by listening, to identify when impulsive sound events occurred. Once these events are noted, a short portion of the audio is downloaded for auditory review. An audit trail tracks who accessed the sensor and who requested the audio search.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

ShotSpotter – not the Boston Police Department – is responsible for determining the location(s) for installation of acoustic sensor(s) that detect gunshot-like sounds and obtaining permission from the premises owner/property manager/lessee.

ShotSpotter utilizes multiple technology and policy protections to protect against audio surveillance:

- Sensors are placed high above the street typically on building or streetlights to avoid street level sounds and the microphones used are not specialized in any way (*i.e*., everyday cell phone quality).
- The system is tuned to listen for loud impulsive sounds that are gunshots or similar to gunshots (fireworks, car backfires) and takes no action on other sounds that would include street level sounds or human voices.
- The sensors store a limited amount of audio locally and that audio is automatically purged every 30 hours.
- Sensors are triggered and an incident 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 has the gunfire and 1 second of audio prior to and after the gunfire to establish an ambient noise level. Audio snippets are typically only a few seconds long unless there is a gun battle.

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

The Boston Police Department does not have access to sensor audio. ShotSpotter purges sensor audio every 30 hours.

If an incident is created and sent to ShotSpotter's Incident Review Center, the short audio snippet is stored permanently for evidentiary purposes as well as to train the machine learning model. Per the NYU's Policing Project recommendation, ShotSpotter only stores one second of pre- and post-incident audio. *See* Privacy Audit & Assessment of ShotSpotter, Inc.'s Gunshot Detection Technology, Prepared by The Policing Project at NYU Law (July 2019), available at: https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/6065e7d81422241f592ce0e5/1617291232883/Privacy%2BAudit%2Band%2BAssessment%2Bof%2BShotspotter%2BFlex.pdf

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

   The Shots Fired dashboard contains information on shooting incidents that did not result in any victim(s) being struck; but occurred in the city of Boston and fall under Boston Police Department jurisdiction. This information may come into the department through a 911 call, a ShotSpotter activation, or an officer on-siting an incident. Shots fired incidents are confirmed when ballistics evidence is recovered, or in the absence of ballistics evidence, there is strong witness or officer corroboration. This information is updated based on analysis conducted by the Boston Regional Intelligence Center under the Boston Police Department Bureau of Intelligence and Analysis. The data is for 2015 forward, with a 7 day rolling delay to allow for analysis and data entry to occur.

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

   All media requests made related to surveillance data from a ShotSpotter will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

   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.

8. **Information and Data-Sharing:**
   a. **How can other City or non-City entities access or use the Surveillance Data?**
   b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
   c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

   No other agencies have direct access to ShotSpotter alerts received by the Department.

   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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

ShotSpotter completed a comprehensive training program for both users and trainers of the Department. 24x7 ShotSpotter support is offered through an online chat feature, or BPD can call toll-free for phone support.

ShotSpotter provides technical consulting, documentation, and training as required.

ShotSpotter owns and maintains the acoustic sensors, therefore, there is no network, installation, or maintenance training is necessary for the Department.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

The Department's ShotSpotter program is managed by a BPD Superintendent.

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

All Boston Police Department use of the ShotSpotter system and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law,

all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department use of the ShotSpotter system and all data will be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix FF: ShotSpotter Technical Proposal for Subscription-Based Gunshot Detection, Location, and Forensic Analysis Service for the City of Boston (dated April 28, 2021)**
- **Appendix GG: ShotSpotter Respond Services Agreement**

*See also* https://www.shotspotter.com/resource-center/

**Department: Boston Police Department**
**Surveillance Technology: Latent Print Unit**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   The Latent Print Unit utilizes devices, hardware, and software to provide services including:
   - Crime scene processing including evidence documentation and collection[1]
   - Latent print processing
   - Latent print comparison
   - Fingerprint Database searches via three AFIS systems

   Automated Fingerprint Identification System (AFIS) 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. The database provides access to known print records for comparison purposes. The LPU utilizes three AFIS database systems:

   - AFIX: local database that contains Boston Police ten print and palm print records. The database was implemented in March 2009 and identifies the candidates list by name.

   - MORPHO/Idemia: state database that contains Massachusetts ten print and palm print records. The database was implemented in June 2013 and identifies the candidates list by a State Identification (SID) Number.[2]

   - Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) (accessed through the state Morpho/Idemia database):[3] federal database that contains federal ten print and palm print records. The database identifies the candidate list by FBI number.

   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#).

   Additional fingerprint technology is utilized by the Crime Scene Response Unit. The CSRU has a mobile fingerprint scanning device that may be deployed when requested to identify persons without identification at area hospitals or the Office of the Chief Medical Examiner.

---

[1] The LPU uses Mideo software for case notes and BEAST (Bar Coded Evidence Analysis Statistics and Tracking) software program which provides Forensic Laboratory Information Management Systems (LIMS) for case management and tracking. These two systems are included within the Department's list of "Software" and subject to the use, access, data protection, retention, public access, info sharing, training, oversight, legal authority, and child rights information therein.

[2] Prior to 2013, the BPD LPU accessed the State's NEC database for searches in the State database.

[3] The LPU does not have a stand-alone terminal that can directly access the federal database. Access is gained through the state terminal.

**Department: Boston Police Department**
**Surveillance Technology: Latent Print Unit**

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

Latent print examinations involve the discovery, development, enhancement, documentation, and preservation of residue impressions deposited by contact of friction ridge skin with an object and the comparison of such impressions to the exemplar reproduction of friction ridge skin known to belong to (a) specific individual(s).

"Latent prints" is a generic term of general acceptance but may refer to any of the following:

- Latent, Patent, and Plastic Impressions
- Fingerprints, Palm prints, and Plantar prints
- Chance Impressions and prints of unknown origin

AFIS 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 AFIS 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.

Latent print images that will be searched, must be calibrated to be 1:1. Descriptions, with pictures, are available in the AFIS workflow guide detailing two techniques for calibrating images for entry into AFIS, and can be utilized as a reference.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   Local AFIS Database (AFIX) Considerations
   AFIX Tracker database retains all Boston Police Department arrests and is maintained by the Crime Scene Response Unit. Records uploaded to AFIX Tracker are also added to the MORPHO state database. The LPU prefers searching in the MORPHO state database due to the higher number of identifications made through this system. AFIX Tracker is only used minimally at the discretion of the Criminalist.

   The AFIX database retains all the search criteria listed above as well as the candidate list(s) generated. This information will be maintained by the database for retrieval if needed.

   State and Federal Databases (MORPHO) Considerations
   The State MORPHO database retains Massachusetts criminal and civilian records and is maintained by the Massachusetts State Police. The State MORPHO AFIS system allows the LPU to gain access to the Federal Database. The Federal database retains US criminal and civilian records and is maintained by the Federal Bureau of Investigation.

   Latent prints searched can be added to the unsolved latent database at the Criminalists' discretion. The candidate list(s) generated should be captured and stored on the Storage Area Network (SAN). Detailed procedures for MorphoTrak can be found in the AFIS workflow guide to include entry of latent prints and obtaining exemplar cards.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Only trained and authorized personnel will be given access to the AFIS databases which are password protected. The list of qualified personnel is maintained in the Quality records.

   The LPU is limited in providing the ranked list of candidate's names generated by the AFIS database(s) per the Massachusetts CORI law. Criminal record information cannot be released. Requests for AFIS candidate list(s) with names must be forwarded to the Legal Department.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   **Electronic Data Protection:** The AFIS databases are password protected. Completed reports, examination checklists, and case correspondence will be saved in the Forensic

Laboratory Information Management Systems (LIMS) under the incident number. The SAN is maintained and routinely backed-up by the Information Systems Group (ISG).

**Evidence Storage in the Forensic Division:** There are dedicated secure spaces for evidence handling and storage. Evidence submitted to the Forensic Division is typically received at one of the Evidence Receiving Windows. The Evidence Receiving Windows are locked whenever they are not attended.

Evidence items are also stored at a secure warehouse which is managed by the Evidence Control Unit of the Boston Police Department. The Latent Print Unit has a secure storage container located in the Evidence Control Unit warehouse that is used for the storage of lifts and is only accessible by Latent Print Personnel.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

All surveillance information in AFIX (local database) and MORPHO (state database) is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022).

For the federal database (IAFIS/NGI), the National Archives and Records Administration (NARA) has approved the destruction of fingerprint cards and corresponding indices when criminal subjects attain 99 years of age, or seven years after notification of death. NARA has determined that automated FBI criminal identification records (rap sheets) are to be permanently retained. Biometrics and associated biographic information may be removed from the IAFIS/NGI earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

The AFIS databases are not public systems.

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests made related to surveillance data will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

A report of results will be completed for all searches against the database. AFIS searches where no hit has been made will not fall under the verification process. 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.

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.

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

All employees in the LPU must complete technical/administrative training programs before assuming responsibilities. Technical staff undergo competency testing before assuming responsibilities. The LPU examiners also undergo annual proficiency tests in each discipline he/she is authorized to perform testing.

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

The Latent Print Unit is accredited by ANAB (ISO 17025:2017, AR 3125).

There were no reported non-conformances in the last full assessment (2021). There were no reported non-conformances in the last surveillance audit (2022).

**Internal Audits:** Internal unit-wide audits are conducted annually in the Latent Print Unit.

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

**AFIS Systems Documentation:** Local (AFIX), State (MORPHO), and Federal (IAFIS) searches will be documented with the date searched. Unique search numbers may be added for each latent searched in the system. A calibrated/cropped latent image for AFIS databases may be stored on the SAN in the appropriate incident number folder.

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    The LPU utilizes devices, hardware, and software, including, but not limited to, the AFIS databases, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    The LPU utilizes devices, hardware, and software, including, but not limited to, the AFIS databases, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation:

- **Appendix BB: Latent Print Unit Standard Operating Procedures Manual**
- **Appendix CC: Latent Print Unit AFIS Workflow Guide**

**Department: Boston Police Department**
**Surveillance Technology: Software and Databases**

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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. A detailed, but non-exhaustive, list of software and databases utilized by the Department is attached. This list includes databases maintained by the Department, databases to which the Department contributes data, and databases the Department accesses to view data.

   Software and databases are used to assist in the investigation of criminal activity in the City of Boston. 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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Depending on the software capabilities and the data and information available within each database, authorized users may perform the following functions on the data in a database: view, add, edit, delete, query, or export/print data.

   Use of software and databases shall be limited to users authorized by the Department to access these tools in the course and scope of their employment to support the administrative and investigatory functions of the Department. All authorized users must have a valid law enforcement, public safety, or administrative purpose for using software and interacting with data in a database maintained by or accessible to the Department.

   All authorized users are required to complete and agree to the BPD Data Use Agreement prior to accessing any database maintained by the Department. Use of databases administered by the Boston Regional Intelligence Center (BRIC) are further governed by and subject to the BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy (2021). Databases not maintained by the Department are subject to the database administrator's user agreements and terms of service.

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

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

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Use of software and databases shall be limited to users authorized by the Department to use the software and access the databases in the course and scope of their employment to support the administrative and investigatory functions of the Department. *See also* BPD Rule 322 (Department Property).

   All authorized users must have a valid law enforcement or public safety purpose for using software and interacting with data in a database maintained by or accessible to the Department. All authorized users are required to complete and agree to the BPD Data Use Agreement prior to accessing any BPD database. Use of databases administered by the BRIC are further governed by and subject to the BRIC Privacy Policy.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

   Databases may contain CJIS Information. The Police Department is audited every three (3) years by FBI CJIS to ensure that we, as a Department, adhere to the standards defined in the Criminal Justice Information Security Policy. The most recent audit was conducted in July 2021. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Boards decisions

along with nationally recognized guidance from the National Institute of Standards and Technology (NIST).

The CJIS Security Policy defines standards for everything from physical security, network security, log file retention, encryption requirements (FIPS 140-2) to security awareness training. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage and destruction of Data. This Policy applies to every individual, contractor, with access to or who maintain and support information services.

6. **Data Retention:**
   a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
   b. **Why is that retention period appropriate to further the purpose(s)?**
   c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

Each database is subject to relevant data retention policies.

Data within BPD-maintained databases is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Data within BRIC-managed databases is further subject to the retention policy in the BRIC Privacy Policy, Section M (Information Retention and Destruction). In particular, the BRIC will review all applicable information for record retention (validation or purge) at least every five (5) years, as provided by 28 C.F.R. Part 23 (Criminal Intelligence Systems Operating Policies). The BRIC conducts quarterly reviews and ongoing maintenance to validate or purge information.

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including,

but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

All media requests will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Authorized users receive training before gaining access to software and databases. The type and manner of training varies based on the complexity and nature of the software, the type and sensitivity of the data and records, and the users' role and responsibility within or relationship to the Department. Training includes, but is not limited to, Boston Police Academy training on report writing and record management system use, training on CORI and CJIS laws and rules, training on Bias-Free Policing and Implicit Bias training. Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

For databases maintained by the BRIC, all BRIC analysts receive at least 40 hours of training per year. New analysts are extensively trained by their supervisors and peers on

all policies and procedures relevant to their roles and responsibilities. Ongoing refresher training is provided to all personnel on a periodic basis as needed.

Analysts are trained in accordance with the Analyst Professional Development Road Map, Version 2.0, produced in 2019 by the U.S. Department of Justice, Bureau of Justice Assistance, the Global Information Sharing Initiative, and the Department of Homeland Security.

Additionally, all BRIC personnel are trained at least annually on the BRIC Privacy Policy and 28 C.F.R. Part 23, as well as all other relevant BRIC policies and standard operating procedures.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

    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.

    For databases maintained by the BRIC, the BRIC will be open with the public in regard to information and intelligence collection practices. The Center's Privacy Policy will be provided to the public for review, made available upon request, and posted to http://www.bpdnews.com and the National Fusion Center Association Web site (http://new.nfcausa.org/).

    The BRIC's Privacy Officer, on behalf of the Privacy Committee, will be 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 center.

    The BRIC will maintain 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.

    The BRIC will adopt and implement procedures to evaluate the compliance of users with the Privacy Policy and with applicable law, to include a review of logging access to BRIC information systems and periodic auditing of user compliance. These audits will be

conducted at least annually, and a record of the audits will be maintained by the Privacy Officer on behalf of the Privacy Committee.

If an Authorized User is found to be in noncompliance with the provisions of the Privacy Policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Bureau Chief of the Boston Police Department's Bureau of Intelligence and Analysis and/or the Director of the BRIC may:
• Suspend or discontinue access to information by the center personnel, the participating agency, or the Authorized User.
• Apply administrative and/or legal actions or sanctions as consistent with Department rules and regulations or applicable law.
• If the Authorized User is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.

Additional details regarding accountability and enforcement are available in the BRIC Privacy, Civil Rights, and Civil Liberties Protection Policy (2021), Section N (Accountability and Enforcement).

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    All Boston Police Department use of software and access to databases and data contained therein shall be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department use of software and access to databases and data contained therein shall be in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting Documentation

- **Appendix DD: List of Software and Databases**
- **Appendix AA: Boston Police Department Data Use Agreement**
- **Appendix Z: Boston Regional Intelligence Center Privacy, Civil Rights, and Civil Liberties Protection Policy (2021)**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Use of specialty cameras and devices shall be limited to only BPD personnel authorized by the Department to deploy the devices in the course and scope of their employment to support the administrative and investigatory functions and community caretaking responsibilities of the Department.

   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).

3. **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

   The specialty cameras and devices include the following:

   - Night vision cameras: still photographs or real-time video, non-recording

   - 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[1]

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   Specialty cameras and devices shall be stored in a secure location, and all access and use of the devices shall be documented in an investigative file. Any still images captured by the devices shall be stored in the physical case file and/or stored within a BPD-approved electronic case/content management system (*i.e.*, "Detective Case Management"). Access to the still images captured by specialty cameras and devices shall be limited to authorized BPD personnel for legitimate law enforcement purposes only. *See also* BPD Rule 322 (Department Property).

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

   BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

[1] The Boston Police Department does not utilize "X-Ray vans."

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

    All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

    Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

    BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

    All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

    All media requests made related to surveillance data from a Department UAS will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

    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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**

b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

9. **Training:**
   a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
   b. **What are the training materials?**

Training on the operation of specialty cameras and devices is provided by the vendors.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

All Boston Police Department specialty cameras and devices shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States

Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department specialty cameras and devices shall be deployed and all data shall be collected, maintained, and utilized in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, including, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

   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 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 technology includes DJI AeroScope Drone Detection Technology 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; 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.

   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).

2. **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

   Boston Police Department Rule 407 governs the use of Department UAS.

   Department UAS may be utilized in situations that include: search and rescue operations; photographic and video deployments; motor vehicle crash investigations and crash scene mapping; criminal investigations and crime scene mapping; tactical response deployments; providing an aerial perspective to assist officers in providing direction for crowd management, traffic incident management, special circumstances, and temporary perimeter security; fire services support; aerial police response deployment; and other special events as assigned by the Commissioner, Superintendent-in-Chief, and/or the Boston Police UAS Manager or designee.

   The UAS Manager shall be assigned to BFS, Homeland Security Unit.

   All Boston Police Department UAS deployments must comply with the United States Constitution, Massachusetts Declaration of Rights, all applicable laws and ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders. If a UAS is deployed for investigative purposes where a person has a reasonable expectation of privacy, it will only be done so pursuant to a search warrant or if exigent circumstances exist. *See also* BPD Rule 334 (Search Warrant Application and Execution).

   To ensure proper documentation of all flights, all UAS deployments must be approved by the UAS Manager and a proper Notice to Airman (NOTAM), in accordance with 14 C.F.R. § 91.139, must be in place.

   Prohibited uses of Department UAS include: to conduct personal business; intimidate, harass, or discriminate against any individual or group; target a person based solely on individual characteristics such as, but not limited to, race, ethnicity, national origin, religion, disability, gender or sexual orientation.

   Department UAS shall not be weaponized nor shall they include facial recognition technology.

   Department UAS are not deployed to create an aerial surveillance program used to continuously record public movements. Department UAS are not used to retain information in order to create a database of recordings that can be retroactively accessed by members of the Department for investigatory purposes unrelated to the initial deployment of the UAS. The use of UAS does not enable the Department to reveal where individuals come and go over an extended period of time, thereby allowing the Department to make deductions from the whole of individuals' movements.

Department UAS are deployed in a manner, as further described below, that minimizes the recording of private places and/or people and forbids the intentionally discriminatory application of laws in the City of Boston.

The use of Department UAS must also comply with all other Department Rules and Procedures, including, but not limited to BPD Rule 113A (Bias-Free Policing Policy). The use of any UAS by the Boston Police Department is strictly prohibited unless it is authorized by the UAS Manager.

In addition to BPD Rule 407, the Department adheres to a 27-page Boston Police Department UAS Operations Manual that ensures Department Personnel use all UAS in a safe, efficient and lawful manner while also taking every reasonable effort to mitigate the invasion of the citizenry's privacy interests during operation. *See* attached as Exhibit B.

**3. Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

All Department UAS are equipped with individual cameras that have the ability to record video footage. The video footage is retained in one of two ways. On most flights, the footage is retained on a memory card. If said footage involves a criminal investigation it is transferred, in its entirety, to an external disc or thumb drive. If the flight is recorded through the FLIR Video Management System, it is retained on the FLIR storage system for a period of thirty days.[1]

None of the cameras can record audio. The Department has two 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 re "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

[1] Flights which are recorded through the FLIR System typically involve emergency situations where it is necessary to provide live feed access to BPD Command elements who are not on scene.

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.

4. **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

   If video footage is recorded under the FLIR camera system, it is retained for a period of thirty days. If a preservation request is not made, the video will automatically delete after the thirty-day retention period. Boston Police Department Telecommunications retains, and has access to, this footage. All requests for this information must be directed to the Video Evidence Unit.

   If the surveillance data is recorded in relation to a criminal investigation the data is transferred to an external storage device and provided to the detective assigned to the investigation. This information is retained in accordance with BPD Rule 331 (Digital Images Collection, Transfer, and Archive Procedures (DICTA)). *See also* BPD Rule 322 (Department Property). The primary investigator assigned is responsible for providing any copies of this data in compliance with discovery obligations.

   Unauthorized use, duplication, and/or distribution of UAS digital media files is expressly prohibited.

5. **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

   All information collected through the use of a Department UAS in relation to a criminal investigation is stored, unencrypted, on an external disk or thumb drive. The disk or thumb drive is maintained in accordance with BPD Rule 331 (Digital Images Collection, Transfer, and Archive Procedures (DICTA)). Access is limited to the primary investigator, who must submit a request for a copy of the information.

   All information recorded under the FLIR camera system is maintained by Boston Police Department Telecommunications. The recordings are unencrypted. Copies of the recordings are only provided if there is a written request made to the Video Evidence Unit or if it is used solely for training purposes. Department personnel requesting utilization of a UAS digital media file for training purposes shall submit the request through the chain of command to the UAS Manager. *See* BPD Rule 101 (Organizational Structure). Recordings may not be copies or sent beyond its training intent without approval of the UAS Manager.

BPD personnel must abide by security terms and conditions associated with all computer systems of the BPD, including those governing user passwords and logon procedures. BPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the BPD, as required in the execution of lawful duty.

BPD personnel are responsible for preventing third parties unauthorized access to information. Failure to adhere to the Department's Data Use Agreement may subject BPD personnel to disciplinary and/or criminal action. BPD personnel must confirm the identity and affiliation of individuals requesting information from the BPD and determine that the release of information is lawful prior to disclosure. Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

6. **Data Retention:**
    a. **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b. **Why is that retention period appropriate to further the purpose(s)?**
    c. **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

All surveillance information is retained in accordance with the Massachusetts Statewide Records Retention Schedule (Revised May 2022) and BPD Rule 322A (Retention and Destruction of Records and Materials).

Any information related to a crime or an investigation of criminal activity must be maintained in accordance with the Schedule and preserved so it can be made available for discovery during the pendency of the case and any subsequent appeals as required of all Public Agencies in the Schedule.

If data stored on a memory card is not required to be maintained pursuant to the Schedule, or if data has been retained for the time period required under the Schedule, it shall not be destroyed unless authorized by the Police Commissioner or the UAS Manager. If data is recorded under the FLIR system, it is retained for a period of thirty days, unless it is preserved.

If a Department UAS is deployed solely for training purposes, and does not contain any information related to a criminal investigation or BPD related mission, the UAS Manager has the discretion to delete the recording. Training flights are conducted in pre-designated, public areas that are chosen based upon airspace classification and minimization of recording individuals.

7. **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

   BPD is committed to accountability and transparency and publicly provides information and data on Dashboards available at: https://www.boston.gov/civic-engagement/boston-police-accountability-and-transparency-data

   The unauthorized use, duplication, and/or distribution of UAS digital media files is expressly prohibited.

   The rules and processes for disclosure of the Surveillance Data is dependent on who is requesting the data, the manner in which the data is being requested, and the contents of the data.

   If the UAS Manager receives the request directly, he or she will determine if an investigator is assigned to the case and coordinate with the investigator for providing all responsive and relevant information. As set out below, access for surveillance data to prosecutors and criminal defendants will be handled in accordance with all relevant rules of criminal procedure.

   All public records requests related to surveillance data will be responded to in accordance with Mass. General Laws ch. 66, and all other applicable laws and regulations, including, but not limited to, BPD Rule 307 (Security of Criminal Offender Record Information (CORI) and The Public Record Law (PRR)).

   All media requests made related to surveillance data from a Department UAS will be directed to the Office of Media Relations and handled in accordance with BPD Rule 300 (Office of Media Relations – Release of Official Information).

   If the surveillance data is relevant to a criminal case or investigation, all discovery requests or subpoenas made by federal and state prosecutors shall be directed to the primary investigator assigned to the case. 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.

8. **Information and Data-Sharing:**
    a. **How can other City or non-City entities access or use the Surveillance Data?**
    b. **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c. **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

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).

The manufacturers of all Department UAS will not have access to any recordings or information that is collected during any Department flights. The UAS Manager may share training videos with UAS manufacturers so long as the information shared does not contain information that is associated with, or capable of being associated with, any identifiable individual or group.

9. **Training:**
    a. **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**
    b. **What are the training materials?**

Department UAS may only be operated by Department pilots who hold a Remote Pilot Certificate issued by the Federal Aviation Administration (FAA) pursuant to 14 C.F.R. Part 107. A Part 107 Certification is a certificate issued by the FAA to individual pilots who have completed an FAA examination that grants permission to fly UAS within specific parameters set forth in 14 C.F.R. Part 107. The UAS Manager ensures that all pilots' training and licensing is compliant with current FAA regulatory requirements.

The primary instructor for Department pilots is the UAS Manager. All Department pilots are provided with a copy of BPD Rule 407, the Department's Certificate of Waiver or Authorization, and the BPD Unmanned Aircraft Systems Operations Manual.

All pilots must attend a Department course and pass a proficiency test established by the UAS Manager. The proficiency test shall be in accordance with Standard Test Methods for Small UAS established by the National Institute of Standard and Technology (NIST) and/or a practical application test established by the UAS Manager. All pilots must complete a quarterly proficiency test, established by the UAS Manager. Failure to pass the proficiency test will result in suspension from the Department's flight program. The

results of the proficiency test must be entered into the pilot's flight record. Additionally, all members of the flight program must conduct at least three flights, to include take-offs and landings, every ninety days. If a pilot does not have any documented training or flight time within a span of ninety days they must meet with the UAS Manager before they can operate a Department UAS. All training will include focusing on the ability to navigate a Department UAS, as safely as possible, while minimizing the recording of private places or citizens who are not the subject of the UAS deployment.

Officers also receive training in the constitutionality of police interactions to reduce the effects of implicit bias and more effectively serve the diverse communities they represent. *See* BPD Special Order 21-25 (Diversity, Equity and Inclusion (DEI) Policy).

10. **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

    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.

    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.

    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).

11. **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

    Boston Police Department UAS are deployed in limited situations delineated in BPD Rule 407. All Department UAS deployments, and any data collection as a result of a deployment, are in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders.

    The Department does not and cannot deploy UAS in a surreptitious manner due to the size and sound of Department UAS and restrictions on where UAS can be operated. The maximum amount of time a Department UAS can remain in flight before having to be recharged is approximately fifty-five minutes due to the physical design constraints of the UAS. If a UAS is deployed for investigative purposes where a person has a reasonable expectation of privacy it will only be done so pursuant to a search warrant or if exigent circumstances exist.

    Surveillance data collected by Department UAS are maintained in a manner that limits access to said information by third parties, but is retained in accordance with all applicable rules of criminal procedure and the Statewide Records Retention Schedule. All Department UAS flights, including training flights, are properly documented and maintained by the Department.

12. **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

    All Boston Police Department UAS shall be deployed, and all data shall be collected, maintained, and utilized, in accordance with the United States Constitution, Massachusetts Declaration of Rights, all applicable federal and state laws and case law, all local ordinances, and all Department Policies, Procedures, Rules, SOPs, and Special Orders, to include any authorities, including but not limited to, Mass. General Laws ch. 119, that may address the protection of information related to juveniles.

## Supporting documentation:

- **Appendix G: BPD Rule 200**
- **Appendix O: BPD Rule 331**
- **Appendix U: BPD Rule 407**
- **Appendix EE: UAS Operations Manual**

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

1. **Purpose: What is the purpose of this Surveillance Technology?**

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

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

Use of the above-referenced technologies is governed by the policies, rules, and regulations referenced in the questionaries submitted for those technologies. The above-referenced technologies which may be deployed in vehicles do NOT have any additional capabilities beyond what is referenced in the questionnaires and relevant attachments.

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).

**Department: Boston Public Schools**
**Surveillance Technology: Cameras and Video Management System**

1) **Purpose: What's the purpose of this Surveillance Technology?**

Cameras are installed in the interior and exterior of school property for the purpose of serving as a safety/security deterrent and also as a recording tool for student/ staff safety. Video surveillance of students captured by BPS cameras is governed by FERPA, IDEA, MGL Ch. 71, Section 37L and 603 CMR 23.00. In addition, student data sharing is governed by Superintendent's Circular LGL-7, Privacy of Student Information and Student Record Procedures: How to Respond to Student Record Requests in Compliance With FERPA and State Law. Please find the BPS policy regarding Superintendent's Circular LGL-7: Privacy of Student Information and Student Record Procedures How to Respond to Student Records Requests in Compliance with FERPA and State Law which encompasses video surveillance of students. Video surveillance that does not include student information, i.e. occurs after school hours, is governed by the Superintendent's Circular LGL-3: Public Records Requests. Access to video surveillance via subpoena is governed by the Superintendent's Circular LGL-5: Subpoenas.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

Authorized use is to monitor the area outside of schools, at entry ways, in certain indoor areas of schools, and on school buses for deterrent and security purposes.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

BPS cameras capture video footage but do not record audio.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Only school officials may access video surveillance data. All requests from third parties, including City of Boston departments and other government agencies, for video surveillance must be reviewed by the Office of Legal Advisor and require a FERPA, IDEA/ Ch. 71, Sec. 37L, 603 CMR 23.00, and BPS Data Sharing Policy Analysis prior to release. Should a request for video surveillance not fit within one of the above-referenced statutes, the request is denied.

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

BPS has physical and cyber security measures in place to protect from unauthorized access to cameras, however BPS' security plan prevents any additional information that could be used to

cause harm from being shared in a public forum. All requests for copies of video footage must go through the Office of Legal Advisor and must fall within federal and state student privacy exemptions for the release of such video.

6) **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b) **Why is that retention period appropriate to further the purpose(s)?**
    c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

BPS adheres to student record data retention requirements under Massachusetts and federal law as well as the MA Statewide Records Retention Schedule.

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

No public access to video footage because much of the video surveillance constitutes FERPA. After hours video of surrounding streets, etc. may be released upon public records requests that are managed through the Office of Legal Advisor. All third party requests, including other City Departments, for video surveillance go through BPS OLA.

8) **Information and Data-Sharing:**
    a) **How can other City or non-City entities access or use the Surveillance Data?**
    b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**
    c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

There is no city-interdepartmental, external government agency, or third party organization access to BPS video surveillance footage because video surveillance may contain student educational records and FERPA, IDEA, and 603 CMR 23.00 govern the sharing of student education record information.. With the exception of state and federal government education agencies (DESE and DOE) whose access to student records is explicitly set forth in FERPA, nn-parent/guardian requests for video surveillance containg student education information cannot be released without 1) parental consent; 2) subpoena or court order; 3) imminent health or safety emergency (which federal guidelines describe as a terrorist attack, active shooter, or pandemic outbreak). With respect to requests for video footage that contains student educational record information from law enforcement (including district attorneys) such requests must comply with FERPA, IDEA, MGL Ch. 71, Sec. 37L, 603 CMR 23.00, and BPS student data sharing circular. Non-law enforcement requests for video surveillance that contain student educational record information require a FERPA, IDEA, 603 CMR 23.00 and BPS policy review prior to disclosure. Video surveillance that does not contain student educational record information as defined by the IDEA, FERPA and 603 CMR 23.00, may constitute public records, subject to exemptions. For

example, after hours video of surrounding streets, etc. may be released upon request and such interdepartmental requests are managed through the Office of Legal Advisor.
Please see response No. 8(a).

9) **Training:**

    a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

One senior official within the BPS Facilities Department has access to cameras and has been trained on use of the system. School leaders may access footage for purposes of searching and reviewing, but are not authorized nor have capabilities to save, download, or share video footage.

    b) **What are the training materials?**

N/A

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

BPS Student Data Policy, BPS Public Records Circular, BPS Subpoena Circular, FERPA, IDEA, Ch. 71, Sec. 37L, 603 CMR 23.00 as well as any other applicable laws that govern the release of information depending on the video images captured. The Boston Public Schools Office of Legal Advisor authorizes the release of video footage to outside parties/agencies based on a case by case determination/review.

11) **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

See No. 10

12) **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

BPS Student Data Policy, BPS Public Records Circular, BPS Subpoena Circular, FERPA, IDEA, Ch. 71, Sec. 37L, 603 CMR 23.00, BPS Student Data Sharing Circular.

**Department: Boston Public Schools**
**Surveillance Technology: Cameras and Video Management System**

## Supporting Documentation:

- **Appendix II: BPS Superintendent's Circular LGL-3: Public Records Requests**
- **Appendix JJ: BPS Superintendent's Circular LGL-5: Subpoenas**
- **Appendix KK: BPS Superintendent's Circular LGL-7: Privacy of Student Information and Student Record Procedures How to Respond to Student Records Requests in Compliance with FERPA and State Law**
- **Appendix LL: BPS Policy Regarding Preparing And Sharing Student Incident Reports And Other Student Information With The Boston Police Department**

**Department: Office of Emergency Management**
**Surveillance Technology: Critical Infrastructure Monitoring System (CIMS)**

1) **Purpose: What's the purpose of this Surveillance Technology?**

The Office of Emergency management (OEM) utilizes cameras that are managed by the Metro Boston Homeland Security Region (MBHSR), a regional network of nine municipalities: Boston, Brookline, Cambridge,[1] Chelsea, Everett, Quincy, Revere, Somerville, and Winthrop. OEM serves as the fiduciary and administrative support to the MBHSR. The MBHSR's cameras make up the Critical Infrastructure Monitoring System (CIMS).

The purpose of CIMS is 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 and otherwise assist officials with the provision of municipal services in order to enhance overall municipal efficiency, and assist with the training of department personnel.

OEM utilizes live video footage from the CIMS cameras during activations of the Emergency Operations Center (EOC) and to maintain situational awareness and a posture of readiness during developing incidents.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

CIMS is governed by MBHSR's CIMS Closed Circuit Television (CCTV) Policy. The MBHSR CIMS Policy is effective upon approval from the MBHSR Jurisdictional Points of Contact (JPOCs). OEM shall maintain the official copy of the approved policy.

Under the direction and oversight of OEM, the JPOC Committee shall be responsible for the revision, update, and distribution of the MBHSR CIMS Policy. The JPOC Committee will ensure that the Policy is reviewed on an annual basis, at a minimum, so that it remains current and operative.

Live camera footage may be displayed on a screen in the EOC Operations Room, managed by OEM, during an activation, visible to all EOC representatives present for the duration of that activation or developing incident. Once the activation is complete, the OEM Boston Police Public Safety Liaison will log out of the camera system, terminating access.

[1] While Cambridge is a part of the MBHSR, it does not participate in the CIMS program.

**Department: Office of Emergency Management**
**Surveillance Technology: Critical Infrastructure Monitoring System (CIMS)**

Viewing of live video footage is only permissible by OEM staff and other approved/vetted representatives participating in an EOC activation, including but not limited to public safety partners, state agencies, and private sector partners that provide services to the City and support the City's response to crises (for example, the American Red Cross). The OEM Police Department Public Safety Liaison or their designee is responsible for providing EOC access to live video footage during an activation or developing incident.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

Cameras are able to collect video, but not audio. Cameras deployed as part of the MBHSR CIMS may have pan-tilt-zoom ("PTZ") or thermal capability. Cameras that are part of the CIMS network shall not utilize facial recognition capabilities if available. Except during an active investigation, jurisdictions shall not utilize automatic identification or automatic tracking capabilities with CIMS cameras.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

The Commissioner/Chief or his/her designee within each jurisdiction will designate the number of System Administrators allowed to grant and oversee access to the CIMS network. Those designated System Administrators have the ability to create groups within their jurisdiction and assign permissions based upon job function or assignment.

Permissions are determined by the System Administrator and include the capabilities to view, rewind, download, or restrict camera footage. System Administrators are designated based upon their subject matter expertise to the MBHSR CIMS program and do not hold operational functions that would create a conflict of interest.

Jurisdictions may utilize the CIMS camera network at local dispatch areas, the front desk of public safety buildings, jurisdictional Emergency Operation Centers (EOCs), or where deemed necessary consistent with the purposes of the CIMS.

When authorized to do so by a jurisdiction, a requesting jurisdiction within the MBHSR will have the ability to view images/video produced by the CIMS cameras of the jurisdiction that has authorized and granted such access. MBHSR jurisdictions will designate that the Police Commissioner/Chief or their designee shall have exclusive authority to authorize other jurisdictions within the MBHSR to view, on an ongoing or time-limited basis and in real time only, footage recorded by the CIMS cameras. Other jurisdictions within the MBHSR may request a copy of archival footage produced by a jurisdiction's CIMS cameras pursuant to the procedures set forth in Section 5.2 of the CCTV policy.

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

**Department: Office of Emergency Management**
**Surveillance Technology: Critical Infrastructure Monitoring System (CIMS)**

Access to the Emergency Operations Center is limited through the use of RFID card readers at all entrances. Representatives from partner agencies/organizations provide names and contact information for all EOC representatives participating in an activation, and EOC representatives are provided with temporary access to card readers to enter the building. Credentials are returned once the activation is completed. The OEM Public Safety Liaison is responsible for logging out of any computer that has access to the camera system at the conclusion of the EOC activation or viewing period.

6) **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**
    b) **Why is that retention period appropriate to further the purpose(s)?**
    c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

No data is retained by OEM. Data may be collected or retained by the BPD or the MBHSR, and policies around collection, access, protection, and retention are governed by those agencies.

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

Live footage observed during an activation is not accessible to members of the general public.

8) **Information and Data-Sharing:**
    a) **How can other City or non-City entities access or use the Surveillance Data?**

Other City or non-City entities are able to view live camera footage during an activation or developing incident at the EOC. Because OEM does not collect or retain data, we do not share information among City agencies or with non-City entities.

During live activations, the BPD generally has a representative present in the EOC to manage live footage.

BPD has automatic access to real-time and recorded footage and retains autonomous authority to share information, according to BPD policies.

    b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

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 (ie; 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. This will

help support audits of the CIMS network and be used to impact future strategic decision making with regards to the CIMS program.

In order to make a request to an MBHSR jurisdiction, all other jurisdictions will utilize a form that will be initially hosted by Boston OEM until individual jurisdictions are able to get a similar version of this form hosted and owned by their own agencies. Once completed, forms will be sent to a jurisdiction's Commissioner/Chief or his/her designated System Administrators to review and either approve or deny the request. Requests made from other law enforcement agencies will be handled by the system administrator themselves, while all requests made from civilians will be sent to a local jurisdiction's legal department for review and input on the request.

c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

As the coordinating department for the City during major planned and unplanned events, viewing of live camera footage is essential to our public safety mandate

9) **Training:**
   a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

OEM staff are trained to participate in emergency activations at the EOC as part of the office on-boarding process via FEMA Incident Command Structure courses. The Boston Police Department is responsible for any training on operation of the camera system by the Public Safety Liaison or Boston Police Department representatives.

   b) **What are the training materials?**

OEM does not provide any training materials and defers to the Boston Police Department for any training materials.

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

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

To ensure transparency and communication with local governments, OEM 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 amount of instances where real-time camera access was granted by a jurisdiction to a requesting agency.

Anyone who engages in an impermissible use of the MBHSR CIMS may be subject to criminal prosecution per M.G.L., civil liability, and/or administrative sanctions, including termination, pursuant to and consistent with the relevant collective bargaining agreements and Department policies.

Violations of this Policy occur when an individual utilizes the MBHSR CIMS network for purposes including but not limited to;

- Invasion of Privacy. Except pursuant to a court order, it is a violation of this Policy to observe, or record footage of, locations except those that are in public view from a vantage point that is accessible to the general public and where there is no reasonable expectation of privacy. Areas in which there is a reasonable expectation of privacy include the interior of private premises such as a home.
- Harassment / Intimidation. It is a violation of this Policy to use the MBHSR CIMS to harass and/or intimidate any individual or group.
- Use / Observation Based on a Protected Characteristic. It is a violation of this Policy to use the MBHSR CIMS to observe individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classification protected by law.
- Personal Use. It is a violation of this Policy to use the CIMS for any personal purpose.
- First Amendment Rights. It is a violation of this Policy to use the MBHSR CIMS for the purpose of infringing upon First Amendment rights.

The Chief of OEM or their designee is responsible for ensuring compliance with the Surveillance Use Policy when the camera network is viewed during an emergency activation or developing incident. Any individual found to be abusing access to the City's camera network via the EOC shall be stripped of their EOC access credentials and disciplined accordingly by the Chief of the Department. Additionally, secondary access credentials for viewing cameras at the EOC are kept in a secured cabinet at the EOC. Login credentials for camera access are provided by the Boston Police Department.

**11) Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

OEM defers to Corporation Counsel and the Boston Police Department in regard to all legal matters related to use of cameras in the City.

**12) Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

OEM defers to the Boston Police Department in regard to legal and or operational considerations specific to the use of cameras and minor children.

**Department: Office of Emergency Management**
**Surveillance Technology: Critical Infrastructure Monitoring System (CIMS)**

## Supporting documentation:

- **Appendix MM: MBHSR CIMS Policy**

**Department: Boston Parks Department**
**Surveillance Technology: Camera**

1) **Purpose: What's the purpose of this Surveillance Technology?**

The Parks Department uses cameras primarily for the protection of Parks Department property, which falls into an exemption under 16-63.3 section b)2.K of the Ordinance. These are installed at the Franklin Park Maintenance Yard and the George Wright Golf Course, and are operated by Boston Municipal Protective Services (BMPS).

Cameras installed in City parks are operated by the Boston Police Department (BPD), and are used for law enforcement purposes.

2) **Authorized Use: What are the uses of this Surveillance Technology that are authorized, the rules and processes required before that use, and the uses that are prohibited?**

Cameras installed in City parks are operated by BPD and are not directly accessible to Parks employees.

3) **Data Collection: What Surveillance Data can be collected by the Surveillance Technology?**

All data collected goes to the Boston Police Telecommunication team.

4) **Data Access: What individuals can access or use the collected Surveillance Data, and what are the rules and processes required before access or use of the information?**

Parks employees may only access data by requesting footage when necessary from the Boston Police. Data is only accessed when responding to cases of vandalism to park equipment and vehicles (for example, stolen catalytic converters on vehicles).

5) **Data Protection: What safeguards protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms?**

Defer to BPD.

6) **Data Retention:**
    a) **What time period, if any, will information collected by the Surveillance Technology be routinely retained?**

Defer to BPD.

    b) **Why is that retention period appropriate to further the purpose(s)?**

Defer to BPD.

c) **What is the process by which the information is regularly deleted after that period has elapsed, and what conditions must be met to retain information beyond that period?**

Defer to BPD.

7) **Public Access: How can collected Surveillance Data be accessed by members of the public, including criminal defendants?**

Defer to BPD.

8) **Information and Data-Sharing:**
   a) **How can other City or non-City entities access or use the Surveillance Data?**

Parks Department employees may access the surveillance data by requesting footage from the Boston Police Telecommunications team. We defer questions about other City or non-City entities accessing data to the Boston Police.

b) **How is the information shared among City agencies or between City agencies and non-City entities and organizations?**

Defer to BPD.

c) **What, if any, required justification and legal standard is necessary to do so, and what obligation(s) are imposed on the recipient of the Surveillance Data?**

Defer to BPD.

9) **Training:**
   a) **What training, if any, is required for any individual authorized to use the Surveillance Data or technology or to access information collected by the Surveillance Technology?**

There is no staff training for Parks Department employees. Our Office Manager is the point of contact with Boston Police when a camera is being installed on Parks property.

b) **What are the training materials?**

N/A

10) **Oversight: What mechanisms ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance**

**with the policy, internal record keeping of the use of the technology or access to information collected by the Surveillance Technology, audit requirements or procedures, technical measures to monitor for misuse, any independent person or entity with oversight authority, and sanctions for violations of the policy?**

Defer to BPD.

11) **Legal Authority: What statutes, regulations, or legal precedents, if any, control the collection, capturing, recording, retaining, processing, interception, analysis, release, or disclosure of Surveillance Data and technology?**

Defer to BPD.

12) **Child Rights: What are the special considerations specific to the Surveillance Technology and Surveillance Data pertaining to minor children?**

Defer to BPD.