New Bedford Police Department
Office of the Chief of Police

871 Rockdale Avenue, New Bedford, MA 02740
Phone: 508-991-6300

Jonathan F. Mitchell
Mayor

Jason Thody
Chief of Police

Derek J. Belong
Assistant Deputy Chief

Scott A. Carola
Assistant Deputy Chief

September 24, 2026

Dear members of New Bedford City Council,

The Police Department supports meaningful City Council oversight of automated license plate readers and other surveillance technology. The ordinance should establish approval for acquisition and funding, clear limits on use and retention, vendor controls, audits, and public reporting. It should not require legislative approval for routine operational decisions or unintentionally regulate ordinary public-safety systems that do not perform automated, persistent tracking.

The ordinance should be revised before adoption. The most significant issues are the breadth of the definitions, mandatory termination of the existing ALPR system, uncertainty surrounding the Privacy and Civil Liberties Impact Assessment, disclosure of exact device locations, restrictions on interagency cooperation, and Council approval requirements that reach routine deployment and configuration decisions. In addition, we are forming a working group that I think could be helpful in making sure this ordinance balances City Council oversight with public safety efficiency and the operation effectiveness of covered technology.

The recommended framework is a division of responsibilities. The City Council would approve the category of technology, the governing standards, contract renewal, and funding. The Police Department would manage deployment, placement, access, investigations, emergency use, and routine configuration within those approved standards.

Provisions the Department Supports:

- A public hearing before the City acquires a new category of surveillance technology or materially expands an existing system.
- A written assessment describing capabilities, purpose, cost, data practices, security, legal issues, and potential effects on civil liberties.
- A short, fixed retention period, with longer preservation only for evidence, litigation, a warrant, a court order, or another lawful purpose.
- Individual user accounts, documented searches, auditable activity, role-based access, training, and meaningful consequences for misuse.
- Contract provisions prohibiting vendor ownership, sale, commercial exploitation, or unauthorized secondary use of City data.
- Regular internal audits, periodic independent review, and public reporting of aggregate information with appropriate redactions.
- Clear disclosure of surveillance technology expenditures in the Police Department budget presented to the City Council.

Concerns and Recommended Revisions:

Definition of Mass Location Tracking Technology

Ordinance Provision: Section A

Concern: The definition covers any system that continuously or systematically records, stores, analyzes, or tracks the movements or whereabouts of members of the public. The ordinance does not define continuously or systematically, does not require automated identification, and does not require that tracking be the system's primary purpose. The definition could therefore reach existing City cameras, body-worn cameras, in-car video, traffic management systems, port-security cameras, fleet GPS, dispatch records, evidence platforms, and other systems that incidentally record a location.

Public safety effect: A broad and uncertain definition could require hearings, assessments, public location disclosures, audits, and Council votes for routine replacement or use of longstanding public-safety equipment. It could also create disagreement over whether an officer may use ordinary camera footage to reconstruct a suspect's movements after a serious crime.

Recommended approach: Limit the definition to technology designed to automatically identify a person or vehicle and aggregate observations across multiple locations or over time. Add explicit exclusions for systems that record a scene but do not perform automated identification or persistent tracking unless that capability is later enabled.

Suggested language:
Mass Location Tracking Technology means a system whose primary purpose is to use automated identification or correlation to create a persistent or substantially comprehensive record of the movements of an identifiable person or vehicle across multiple locations or over time. The term does not include ordinary fixed security video, body-worn cameras, in-car video, traffic-signal or traffic-engineering systems, City fleet management, emergency communications, access-control systems, evidence-management systems, cybersecurity logs, or cameras used for facility, port, or event security, unless automated identification or persistent tracking functionality is enabled.

Definition of Automated License Plate Reader

Ordinance provision: Section A

Concern: The proposed definition includes any technology that uses automated means to obtain vehicle information or information concerning a vehicle's location or movement. This could include systems that detect vehicles for traffic flow, parking management, gate access, or other no investigative functions.

Public safety effect: An overinclusive definition may subject unrelated municipal systems to police-specific restrictions and approval procedures.

Recommended approach: Define ALPR by its automated capture and processing of license plate characters or searchable vehicle images for identification or investigative use. Exclude systems that merely detect vehicle presence or traffic volume and do not retain identifiable plate information.

Suggested language:
Automated License Plate Reader means a camera and associated software that automatically captures or processes an image of a license plate or searchable vehicle characteristics and creates a record that may be used to identify or locate a vehicle. The term does not include a device that

detects only vehicle presence, count, speed, or traffic flow without retaining identifiable license plate information.

Definition of Material Modification

Ordinance provision: Section A

Concern: The definition treats any expansion in device number or geographic coverage as material. It could include replacing a failed camera, moving one camera in response to construction, adding temporary coverage for a credible threat, applying a security patch, or changing authorized personnel after an assignment change.

Public safety effect: Requiring a hearing, impact assessment, location disclosure, and Council vote for routine adjustments would delay operations and reduce the Department's ability to respond to changing crime patterns and emergencies.

Recommended approach: Reserve Council approval for changes that substantially alter the approved purpose, data collected, retention period, or overall scale. Exclude maintenance, replacement, relocation, cybersecurity improvements, temporary emergency deployments, and personnel changes within an approved access class.

Suggested language:
Material Modification means a change that substantially expands the approved purpose of a covered system, adds a materially different category of data, increases the maximum retention period, or increases the number of deployed devices by more than 25 percent during a fiscal year. It does not include maintenance, replacement with substantially equivalent equipment, relocation of an existing device, cybersecurity or reliability improvements, temporary emergency deployment, or changes in authorized personnel consistent with approved policy.

Existing ALPR Systems and Agreements:

Ordinance provision: Section C

Concern: The ordinance directs the Administration to terminate or allow the existing ALPR agreement to expire and then discontinue the system. This requirement applies even if the existing system can meet every new privacy, security, audit, and transparency standard.

Public safety effect: Mandatory termination could create a more extensive investigative gap, strand an existing investment, interrupt active cases, and remove a capability used for stolen vehicles, violent crime, missing people, and endangered persons without first identifying a compliant replacement.

Recommended approach: Allow the existing system to continue for a defined compliance period. Require the Administration and Police Department to submit the governing policy, impact assessment, contract protections, and budget disclosure within 60 to 90 days. Council could then approve continuation, require changes, or direct an orderly transition.

Suggested language:
An ALPR system in operation on the effective date may continue during a 90-day compliance period. Within that period, the Administration shall submit the materials required by this section. The system may be renewed or continued upon an affirmative vote of the City Council. Nothing in this subsection

requires interruption of an active investigation, destruction of evidence, or termination before the Council completes its review.

Privacy and Civil Liberties Impact Assessment:

Ordinance provision: Section E

Concern: The ordinance requires an assessment but does not identify who prepares it, who supplies technical and operational information, who reviews its legal conclusions, what methodology applies, how it is paid for, or how often it must be updated. It also does not distinguish public content from sensitive security or investigative information.

Public safety effect: An undefined process may produce delay, inconsistent standards, duplication, or a document prepared without sufficient technical, legal, cybersecurity, or operational knowledge. Public disclosure of sensitive details could expose system vulnerabilities or investigative methods.

Recommended approach: Assign preparation to the department proposing the technology, with required participation by City information technology and review by Corporation Counsel. Permit the Mayor or Council to request outside technical or civil liberties review when justified. Establish a standard form, a deadline, and rules for confidential appendices.

Suggested language:
The department proposing the technology shall prepare the assessment in consultation with the City's information technology and cybersecurity personnel. The City Solicitor shall review the assessment for legal sufficiency. The assessment shall use a standard form approved by the Administration and shall be completed within 60 days after sufficient vendor and operational information is available. Information exempt from disclosure by law, including security architecture, credentials, exact investigative methods, and information that could compromise an active investigation, may be included in a confidential appendix available to authorized reviewers.

Public Disclosure of Device Locations:

Ordinance provision: Section F and Section N

Concern: The ordinance requires public disclosure of every proposed location, the reason supporting each location, every relocation, and annual reporting of deployed locations.

Public safety effect: Exact location disclosure provides a map for evasion, vandalism, obstruction, or tampering. It may reveal investigative priorities, sensitive infrastructure, coverage gaps, or temporary deployments addressing a threat. Requiring advance disclosure of every relocation also prevents prompt operational response.

Recommended approach: Disclose the number of devices, general deployment areas, objective placement criteria, and categories of locations. Permit withholding of exact locations when disclosure could compromise public safety, security, an investigation, or system integrity. Allow the Chief to relocate approved devices without another hearing.

Suggested language:
The City shall publicly disclose the number of devices, the general geographic areas or categories of locations in which they are deployed, and the objective criteria used for placement. Exact device locations may be withheld when the Chief of Police and City Solicitor determine that disclosure could

create a risk of evasion, vandalism, interference, or compromise of public safety, infrastructure security, or an investigation. Relocation of an existing device within the approved system does not require a new public hearing or Council vote.

Search Standards and Authorized Uses:

Ordinance provision: Section G

Concern: A documented case number and legitimate law-enforcement purpose are useful controls, but the ordinance does not define authorized purposes, the evidentiary threshold, emergency searches, hot-list alerts, quality assurance, audits, or training. The wording could be interpreted either too broadly or too narrowly.

Public safety effect: Ambiguity can permit inconsistent use or prevent urgent action when no case number has yet been assigned, such as an active abduction, Amber or Silver Alert, suicidal person, or immediate threat.

Recommended approach: Require a documented lawful purpose and reasonable suspicion for historical investigative searches involving a person or vehicle, while defining exceptions for emergencies, missing or endangered people, stolen vehicles, judicial process, system testing, audits, and required maintenance. State that an ALPR result is an investigative lead requiring independent validation.

Suggested language:
A historical investigative search associated with an identifiable person or vehicle shall be supported by documented reasonable suspicion and a case or incident number. This requirement does not prevent a documented search or alert involving an imminent threat, missing or endangered person, stolen vehicle, active BOLO, warrant, court order, victim-reported incident, system audit, training exercise using approved test data, or maintenance. No enforcement action shall be based solely on an automated alert without visual confirmation and an independent lawful basis.

External Sharing and Regional Investigations:

Ordinance provision: Sections G and I

Concern: The ordinance generally prohibits voluntary access or disclosure to federal agencies, out-of-state agencies, private entities, or other external entities unless specifically authorized or required by law. Other external entities could include nearby Massachusetts departments, task forces, prosecutors, schools, hospitals, or agencies assisting with a regional emergency.

Public safety effect: Violent offenders, stolen vehicles, abductors, and missing people cross municipal and state boundaries. A rule requiring legal compulsion before any voluntary sharing may delay urgent investigations and isolate New Bedford from regional partners.

Recommended approach: Prohibit bulk or unrestricted external access by default but allow case-specific sharing with an authorized agency for a documented criminal investigation, missing-person matter, imminent threat, or other defined public-safety purpose. Require equivalent use restrictions, logging, and auditing. Preserve a specific prohibition on civil immigration enforcement if that is the Council's policy choice.

Suggested language:
City ALPR data shall not be made available through unrestricted or indiscriminate external access. Case-specific data may be shared with an authorized law-enforcement or public-safety agency for a documented criminal investigation, missing or endangered person, imminent threat, judicial process, or mutual-aid response, provided the recipient agrees to use the data only for the stated purpose and to comply with applicable retention and disclosure restrictions. Emergency sharing shall be documented and reviewed by a supervisor as soon as practicable.

Independent Audit and Public Reporting:

Ordinance provision: Sections J and N

Concern: The ordinance does not define independent, identify the auditor, establish access to confidential records, allocate cost, or specify whether public reports may omit details that would identify officers, victims, witnesses, investigative targets, security measures, or active cases.

Public safety effect: An undefined audit mandate may be difficult to procure and may expose protected information. Annual review alone is also insufficient to identify misuse promptly.

Recommended approach: Require monthly internal audits by Professional Standards or another unit independent of routine users, plus an annual independent review by the City Auditor, a qualified external auditor, or another entity designated by the City Solicitor and Administration. Public reports should contain aggregate results and legally required redactions.

Suggested language:
The Police Department shall conduct monthly compliance audits through its Professional Standards function or another unit not responsible for routine operation of the system. At least annually, the City Auditor or a qualified independent reviewer designated by the Administration and City Solicitor shall examine compliance. Public reports shall present aggregate findings and corrective actions and shall omit information protected by law or reasonably likely to compromise safety, security, privacy, or an investigation.

Affirmative Council Approval:

Ordinance provision: Section K

Concern: The section requires a Council vote before acquisition, deployment, renewal, expansion, or material modification. When read with the current definitions, it could place individual deployment decisions and routine technology management before the Council.

Public safety effect: Legislative approval for operational changes can delay time-sensitive responses and blur accountability between the Council's policy and the Chief's responsibility for police operations.

Recommended approach: Require Council approval for initial acquisition, contract renewal, a new category of covered technology, or a material modification as narrowly redefined. Preserve the Chief's authority over individual locations, temporary deployments, system configuration, and personnel access within approved policy and funding.

Suggested language:
City Council approval is required before the initial acquisition of a covered technology, renewal of the principal vendor agreement, addition of a materially different capability, or Material Modifications as defined in this section. Within an approved appropriation and governing policy, the Chief of Police retains authority over individual deployment locations, relocation, temporary emergency deployment, user authorization, and routine system configuration.

Vendor Data Disposal and Evidence Preservation:

Ordinance provision: Sections L and M

Concern: The ordinance requires all City data to be exported to the City when a contract ends while also requiring deletion. Exporting every record conflicts with data minimization and creates a new City-held repository. It is not clear that the City has the capacity to receive this amount of data. Literal deletion from disaster-recovery backups may also be technically impossible before normal backup rotation.

Public safety effect: Unnecessary export could extend retention beyond the period approved by the Council. The export of data could also increase the risk of a data breach.

Recommended approach: Consult with the Director of Management Information Systems (MIS), John Costa, on best practices to achieve this goal. Transfer only records that the City is legally required or authorized to preserve, including evidence and litigation holds. Require verified deletion of all other data from active systems and deletion or permanent inaccessibility through the vendor's documented backup cycle.

Suggested language:
Upon termination, the vendor shall transfer only City data subject to an active evidentiary preservation, public-record retention requirement, litigation hold, warrant, court order, or other lawful preservation obligation. All remaining City data shall be deleted from active systems. Residual backup copies shall remain inaccessible for operational use and shall be permanently deleted through the vendor's documented backup-rotation schedule.

Budget Transparency:

Ordinance provision: Recommended addition

Concern: The ordinance requires public cost information during the approval process and annual reporting, but it does not establish a consistent budget presentation for surveillance technology.

Public safety effect: Council oversight is more effective when members can identify the technology, vendor, purpose, recurring cost, and contract term during the ordinary budget process rather than discovering it only after procurement.

Recommended approach: Add a dedicated line item or budget appendix for covered surveillance technology. The disclosure should be specific enough for fiscal oversight without revealing exact locations, network architecture, credentials, or investigative methods.

Suggested language:
The Police Department's annual budget submission shall separately identify each covered surveillance technology or include a surveillance technology appendix stating the technology category, vendor,

authorized purpose, number or approved range of devices, annual operating cost, proposed capital cost, funding source, and contract term. The public budget shall not disclose information that would compromise cybersecurity, exact operational placement, officer safety, or an active investigation.

Emergency Authority and Continuity of Operations:

Ordinance provision: Recommended addition

Concern: The ordinance contains no general emergency provision for an imminent threat, critical incident, major event, infrastructure emergency, or urgent missing-person investigation.

Public safety effect: A system designed for ordinary approval timelines may prevent temporary, narrowly tailored action when delay threatens life or public safety.

Recommended approach: Authorize temporary emergency deployment or access by the Chief or designee for a limited period, with written justification, logging, after-action review, and prompt notice to the Mayor and Council leadership.

Suggested language:
When the Chief of Police or designee reasonably determines that temporary use is necessary to address an imminent threat to life, a critical incident, a missing or endangered person, or a declared emergency, the Department may temporarily deploy or access covered technology for up to 30 days. The use shall be documented, limited to the emergency purpose, audited, and reported to the Mayor and City Council President within five business days, subject to lawful redactions.

In consultation with the City Solicitor, the following legal concerns were also identified:

Section C 1- As written, required modification of existing contract constitutes a breach if not agreed upon by vendor.

Section C 2- Although legally permissible, unilateral termination of current agreement constitutes a breach and entitles vendor to contract damages.

Section H- Requirements of proposed contract would constitute breach of existing contract. Needs to apply prospectively and not to current agreement.

Section L- Application of this provision to termination of current agreement is also a breach of contract. Needs to apply prospectively and not to current agreement.

Section M- Application of this provision to termination of current agreement is also a breach of contract. Needs to apply prospectively and not to current agreement.

Implementation Recommendations:

- Provide a 90-day implementation period rather than making all provisions operational immediately upon passage.
- Direct the City Solicitor to review the final ordinance for consistency with state law, collective bargaining obligations, public-record requirements, evidentiary preservation, procurement law, and the legal authority of the Mayor, Council, and Police Department.

- Adopt a Council-approved governance framework and require the Police Department to publish a detailed operating policy consistent with that framework.
- Require initial and annual training for every authorized user, with immediate suspension of access for noncompliance.
- Establish an annual review meeting at which the Department presents aggregate use, audit findings, violations, corrective action, documented public-safety outcomes, and proposed changes.
- Allow the working group to be formed, evaluate the current conditions, and make recommendations relative to this ordinance and the process moving forward.
- Include a severable process for approving a different vendor without interrupting active investigations or the City's ability to locate a missing or endangered person.

Conclusion:

The Department supports enforceable privacy, transparency, and accountability standards. Council approval of funding and major capabilities is appropriate. Public reporting, short retention, documented searches, audits, training, and vendor restrictions will strengthen public trust.

The ordinance should also preserve the Police Department's ability to respond promptly, work with authorized partners, protect sensitive locations, and manage established public-safety systems. Narrower definitions, a defined assessment process, protected location information, case-specific sharing, operational exceptions, the ability to form and leverage the advice of a working group, and a reasonable transition period would provide meaningful oversight without creating unnecessary risk or delay.

These recommendations are offered from a law-enforcement and public-safety perspective. The City Solicitor should review final language for legal sufficiency and consistency with applicable law before adoption.