

SURVEILLANCE TECHNOLOGY OVERSIGHT
PROPOSED BY-LAW

SECTION 1. AUTHORITY

This by-law shall be enacted pursuant to the Town's home rule authority under Article 89 of the Amendments to the Massachusetts Constitution, M.G.L. c. 43B (the Home Rule Amendment) and M.G.L. c. 40, § 21, which authorizes towns to make reasonable regulations for the protection of persons and property, the preservation of the public health, safety, and welfare, preserving peace and good order, and maintaining their internal police.

This by-law shall also adhere to the Cohasset Town Manager Act (Chapter 34 of the Acts of 1997); M.G.L. c. 41 § 97A (Police Departments, Chief of Police, Powers and Duties); M.G.L. c. 30B (Uniform Procurement Act); M.G.L. c. 66 (Public Records), M.G.L. c. 66A (Fair Practices); M.G.L. c. 214 § 1B (Right of Privacy), and other state or federal law.

SECTION 2. PURPOSE

The purpose of this by-law is to:

- (a) Protect the privacy, civil liberties, and constitutional rights of persons in the Town of Cohasset;
- (b) Ensure that informed public debate occurs as early as possible about decisions related to Surveillance Technology;
- (c) Establish a clear process for democratic review, approval, and oversight of such Surveillance Technology; and
- (d) Require ongoing transparency and accountability for any Surveillance Technology that is authorized.

SECTION 3. DEFINITIONS

For purposes of this by-law, the following definitions apply:

- (a) "*Covered Entity*" means any Town department, board, committee, commission, officer, employee, agent, or contractor acting on behalf of the Town, as well as any private party deploying Surveillance Technology on public property or rights-of-way within the Town.
- (b) "*Select Board*" means the duly elected members of the executive governing body for the Town of Cohasset, who exercise their authority through formal board votes at noticed public meetings.

Town of Cohasset
Sponsor Draft - Citizen Petition

(c)“*Surveillance Technology*” means any system, device, hardware, software, database, method, machine learning or artificial intelligence that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information specifically associated with, or capable of being associated with, any identifiable individual or group; or any system, device, cloud-based platform, database, third party service, software mobile system or vehicle that is capable of collecting, analyzing or recording data about individuals in ways that enable the determination or verification of their identity, location or movements. Surveillance Technology includes, but is not limited to: (i) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (ii) automatic license plate readers, which includes any system, device, camera, or software, fixed or mobile, that uses optical character recognition, machine learning, artificial intelligence, or any other automated process to capture, read, decode, or record vehicle license plate numbers, registration information, vehicle descriptions, or associated metadata; (iii) biometric surveillance technology, including facial, voice, iris, and gait-recognition devices, systems, software and databases; (iv) gunshot detection systems; (v) mobile DNA capture technology; (vi) surveillance enabled or capable lightbulbs or light fixtures; (vii) video analytics software, including social media monitoring software; (viii) social media monitoring software; and (ix) predictive policing software. The enumeration of surveillance technology examples in this subsection shall not be interpreted to exclude from the definition any technology that is not listed but otherwise meets the definition of Surveillance technology.

(d)“*Surveillance Technology*” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a Surveillance Technology as defined in Section 3(c): (i) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or surveillance-related functions; (ii) Parking Ticket Devices (PTDs) however, that PTDs shall not include automated parking enforcement systems that utilize a camera, and related databases, whether the system generates tickets or otherwise; (iii) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (iv) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (v) municipal agency databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; (vi) manually-operated technological devices that are used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (vii) card readers and key fobs used

Town of Cohasset
Sponsor Draft - Citizen Petition

by municipal employees and other authorized persons for access to town-owned or controlled buildings and property; (viii) security cameras including closed circuit television cameras installed by the town to specifically monitor cash-handling operations and to maintain the safety of town employees and visitors to such areas; and (ix) cameras installed solely to protect the physical integrity of town infrastructure. The enumeration of these exclusions shall not be interpreted as an endorsement or approval of their use by any municipal entity.

(e) "*Data*" means any image, record, file, or information collected, generated, or derived through the use of Surveillance Technology, including, license plate numbers, timestamps, GPS coordinates, other geospatial information, photographs, audio recordings, video recordings, any associated vehicle or personal information, and all associated metadata.

(f) "*Exigent Circumstances*" means the Police Chief's good faith and reasonable belief that an emergency involving danger of death, physical injury, or significant property damage or loss, requires the use of the Surveillance Technology or the Data it provides. The use of Surveillance Technology in Exigent Circumstances shall not infringe upon an individual's right to peacefully protest or exercise other lawful and protected constitutional rights.

(g) "*Open Town Meeting*" means a duly called and noticed town meeting of the Town of Cohasset open to all registered voters of the Town, consistent with M.G.L. c. 39.

(h) "*Town Manager*" means the Town of Cohasset's chief municipal administrator and financial officer, consistent with the Cohasset Town Manager Act (Chapter 34 of the Acts of 1997).

(i) "*Viewpoint-based*" means targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

SECTION 4. PROHIBITION

(a) General Prohibition. No Covered Entity shall acquire, deploy, operate, contract for, or otherwise use any Surveillance Technology within the Town without prior express authorization by a majority vote of the Town of Cohasset Select Board as provided in Section 5 of this by-law.

(c) Third-Party Deployment. No private party shall deploy Surveillance Technology on Town-owned property, public streets, public ways, or public rights-of-way within the Town without authorization by the Select Board as provided in Section 5.

Town of Cohasset
Sponsor Draft - Citizen Petition

(d) Indirect Use Prohibited. No Covered Entity shall obtain Data collected by Surveillance Technology from any other jurisdiction, agency, or third party in a manner that circumvents the requirements of this by-law.

SECTION 5. AUTHORIZATION PROCEDURE

(a) Petition for Approval. Any Covered Entity may petition the Select Board for approval by submitting Required Disclosures as required by Section 5(c) to the Town Manager, who will petition the Select Board for approval on the Covered Entity's behalf, prior to engaging in any of the following:

- 1) Seeking funds for new surveillance technology, including but not limited to applying for a grant, or soliciting or accepting state or federal funds or in-kind or other donations;
- 2) Acquiring or borrowing new surveillance technology, whether or not that acquisition is made through the exchange of monies or other consideration;
- 3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the Select Board in accordance with this bylaw, including the sharing of surveillance data therefrom; or
- 4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share, or otherwise use surveillance technology or surveillance data.

(b) Public Hearing. Approval of any petition submitted to the Select Board by The Town Manager on behalf of any Covered Entity is subsequent to a properly noticed public hearing at which the public is afforded a fair and adequate opportunity to provide online, written, and oral testimony for a period of twenty (20) business days both prior to and after the Public Hearing.

(c) Required Disclosures. As part of the process of seeking Select Board approval to fund, acquire, or use surveillance technology or enter into an agreement concerning such funding, acquisition, or use, the Covered Entity shall submit to the Select Board and make publicly available a written **Disclosure Statement** concerning the technology at issue. No use of surveillance technology shall be permitted without the Select Board's express approval of the related Disclosure Statement. Prior to a vote, the Select Board may request revisions be made by the Covered Entity. All revisions must be disclosed and discussed at a Public Hearing, pursuant to Sections 5(b) and 5(c) of this by-law, prior to final authorization of any surveillance technology.

The Disclosure Statement shall include, at minimum:

- 1) a **Surveillance Use Policy** that includes, at a minimum:
 - i) A detailed description of the specific Surveillance Technology and how it works, including the vendor, model, and technical capabilities;
 - ii) A map of the specific locations where the Surveillance Technology would be deployed;

Town of Cohasset
Sponsor Draft - Citizen Petition

- iii) The specific purposes and intended uses of the Surveillance Technology;
 - iv) A detailed description of the rules that will govern the use of the Surveillance Technology, including but not limited to the legal standard that must be met before the Surveillance Technology is used;
 - v) A description of the data to be collected, captured, recorded, or intercepted, including the type of data, retention period, and storage location;
 - vi) How and under what circumstances the surveillance data that was collected, captured, recorded, or intercepted will be analyzed and reviewed;
 - vii) The identities of all third parties, including vendors and other governmental agencies, that would have access to the data with each entity identified by its specific agency, department, or office name, including any sub-unit or field office where applicable, and not by general category;
 - viii) A full copy of any proposed contract or terms of service with a vendor;
 - ix) A description of data security measures and protocols, including safeguards that protect information from unauthorized access such as encryption, access-control, and access-oversight mechanisms;
 - x) The estimated cost of the Surveillance Technology over the one (1) year authorization period, including acquisition, operation, maintenance, and any data storage fees;
 - xi) How the petitioner will comply with its obligations pursuant to the Massachusetts Public Records Law and any other applicable law, regulation, or order of a court or state or federal administrative agency of competent jurisdiction that requires the disclosure of particular surveillance data;
 - xii) The training required for any individual authorized to use the Surveillance Technology.
- 2) A **Surveillance Impact Report** addressing the effect of the Surveillance Technology on the civil liberties and civil rights of Town residents, including but not limited to:
- i) Potential disparate or adverse impacts on any communities or groups if the Surveillance Technology was used or deployed, intentionally or inadvertently, in a viewpoint-based manner;
 - ii) Potential disparate or adverse impacts on any communities or groups if the Surveillance Technology is operated using intentionally or inadvertently biased algorithms;
 - iii) Potential adverse impacts on privacy and anonymity rights;
 - iv) Other potential adverse impacts on the civil rights and civil liberties guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution and the Massachusetts Constitution and state law;

Town of Cohasset
Sponsor Draft - Citizen Petition

- v) What specific, affirmative measures will be implemented to safeguard the public from each of the potential disparate and adverse impacts identified pursuant in the privacy impact assessment;
 - vi) What potential capabilities and uses of the Surveillance Technology will be prohibited, such as the warrantless surveillance of public events and gatherings; and
 - vii) What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and what internal personnel will be assigned to receive, register, track, and respond to such communications.
- 3) Proposed policies governing access to, use of, and retention of data, including audit and oversight mechanisms;
 - 4) A disclosure of the fiscal impact of the Surveillance Technology, including but not limited to initial acquisition costs, ongoing operational costs (including personnel, legal compliance, use auditing, data retention and security costs), and any current or potential sources of funding; and
 - 5) A plain language, non-technical summary document for residents to glean a full picture of what is being proposed without having extensive background or professional knowledge of the law or proposed technology.

(d) Public Disclosure. The public hearing required pursuant to Section (b) may not be held until the required Surveillance Use Policy and Surveillance Impact Report have been available to the public, at a designated page on the Town website, for a period of at least twenty (20) business days.

(e) Standard for Approval. The Select Board shall only approve a request to fund, acquire, or use a surveillance technology if it determines the benefits of the surveillance technology outweigh its costs, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based on discriminatory or viewpoint-based factors or have a disparate impact on any Town community or group. All approved Disclosure Statements shall be made available to the public, at a designated page on the relevant Covered Entity's public website and conspicuously posted at Town Hall for as long as the related surveillance technology remains in use. An approval for the funding, acquisition and/or use of a surveillance technology by the Select Board, where the risk of potential adverse impacts on civil rights or civil liberties has been identified in the Surveillance Impact Report pursuant to Section 5(c)(2) of this by-law, shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impact exists and must be proactively avoided.

(f) Fiscal Impact. Where a petition for approval includes a funding request, the Town Manager shall provide a copy of the written Disclosure Statement pursuant to Section 5(c) to the Select Board, the Advisory Committee, and the Capital Budget Committee, so that the Advisory

Town of Cohasset
Sponsor Draft - Citizen Petition

Committee and Capital Budget Committee may make any recommendation to Town Meeting or the Select Board that it deems appropriate under M.G.L. c 39 § 16 and the General By-Laws.

(e) Scope of Authorization. Each authorization shall be limited to:

- (1) A specific Surveillance Technology or system as described in the disclosure statement;
- (2) Specific locations identified in the Disclosure Statement;
- (3) A defined period not to exceed one (1) year, after which reauthorization shall be required under the same process;
- (4) The specific purposes identified in the Disclosure Statement; and
- (5) Data retention limits and access restrictions as approved by the Select Board.

(f) Modification. Any material change to an authorized use of Surveillance Technology, including, but not limited to, expansion of deployment locations, relocation of existing technologies, expansion of categories of data collected, use of collected data for purposes beyond those initially approved, extension of the retention period, addition of new data-sharing partners, or change in vendor, shall require a new approval from the Select Board, following a Public Hearing and Disclosure, pursuant to Sections 5 (a) and (c) of this bylaw, respectively.

(h) Exigent Circumstances. Notwithstanding the provisions of this bylaw, the Chief of Police may temporarily use Surveillance technology in Exigent Circumstances for a period not to exceed thirty (30) days without following the provisions of authorization before that use. However, if the police department uses Surveillance Technology in Exigent Circumstances under this section, the Chief of Police must:

- (1) Report that use to the Select Board in writing within thirty (30) days following the end of those Exigent Circumstances;
- (2) Submit a Surveillance Impact Report and, if necessary, a technology-specific Surveillance Use Policy to the Select Board regarding that Surveillance Technology within thirty (30) days following the end of those Exigent Circumstances; and
- (3) Include that Surveillance Technology and, if applicable, Surveillance Use Policy, in the next Annual Town Report.

Any Surveillance Technology Impact Report and, if necessary, technology-specific Surveillance Use Policy submitted to the Select Board under this section may be redacted to the extent required to comply with an order by a court of competent jurisdiction, or to exclude information that, in the reasonable discretion of the Chief of Police, if disclosed, would materially jeopardize an ongoing investigation or otherwise represent a significant risk to public safety and security provided, however, that any information redacted pursuant to this paragraph will be released in

Town of Cohasset
Sponsor Draft - Citizen Petition

the next Annual Town Report following the point at which the reason for such redaction no longer exists.

SECTION 6. DATA GOVERNANCE REQUIREMENTS

Any Surveillance Technology authorized under Section 5 shall be subject to the following data governance requirements, which shall be incorporated into the terms of any authorization and any vendor contract:

- (a) Retention Limits. Data collected through Surveillance Technology shall be retained for no longer than fourteen (14) calendar days, unless a longer period is expressly required by a court order, in which case the data relevant to that investigation may be preserved.
- (b) Access Restrictions. Access to Data shall be limited to authorized personnel for the specific purposes approved by the Select Board. Data shall not be accessed for general investigative browsing, immigration enforcement, or any purpose not expressly authorized.
- (c) No Unauthorized Sharing. Data shall not be shared with any department or agency of the Federal government, state agency, state or local law enforcement agency, or third party not identified in the disclosure statement approved by the Select Board, except pursuant to a valid court order or warrant. Furthermore, prior to sharing any data, the Select Board shall ensure that data that is shared is not subsequently shared by the party that the Town of Cohasset is sharing with that would result in the data being shared with any department or agency of the Federal government, state agency, law enforcement agency, or third party not identified in the disclosure statement approved by the Select Board.
- (d) Audit Logs. A complete and tamper-evident audit log of all access to and use of Data shall be maintained and shall be available for public inspection upon request.
- (e) Vendor Contracts. Any contract with a vendor of Surveillance Technology shall:
 - (1) Prohibit the vendor from using, selling, sharing, or retaining any data for any purpose other than providing services to the Town of Cohasset, shall provide for Town ownership of all Data, and shall prohibit licensing or other uses of the data by the vendor;
 - (2) Require that upon termination of the contract, that the vendor of Surveillance Technology to delete or return all surveillance data; provide the Town of Cohasset with audit-log access sufficient to satisfy the reporting in Section 7; and refrain from using Town-collected data for the vendor's own commercial or product development purposes without express written Select Board authorization; and
 - (3) Limit contract or contract renewal for Surveillance Technology to (1) year or be subject to prior Town Meeting authorization pursuant to M.G.L. c 30B § 12, in addition to the Select Board approval required under Section 5 of this by-law.

Town of Cohasset
Sponsor Draft - Citizen Petition

SECTION 7. ANNUAL REPORTING

- A. Annual Reporting. The Covered Entity responsible for any authorized Surveillance Technology shall submit to the Select Board, and make available on both its public website and the Select Board website, an Annual Surveillance Report for each specific surveillance technology used by the Covered Entity within twelve (12) months of Select Board approval, and annually thereafter on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:
- (1) A summary of how the surveillance technology was used;
 - (2) Whether and how often collected surveillance data was shared with any external persons or entities, the names of any recipient person or entity, the types of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosures;
 - (3) Where applicable, a breakdown of where the surveillance technology was deployed geographically, how many individual days the surveillance technology was deployed, what percentage of those daily-reported deployments were subject to (i) a warrant, and (ii) a non-warrant form of court authorization; and what percentage of the reported monitoring was subject to (i) a warrant, and (ii) a non-warrant form of court authorization;
 - (4) Where applicable, a breakdown of how many times the surveillance technology was used to investigate potential or actual (i) violent crimes, (ii) non-violent crimes, (iii) felonies, (iv) misdemeanors, and (v) other legal or code violations, infractions not classified as felonies or misdemeanors, unlawful activity, activities or patterns considered to be indicators of potential future involvement in criminal activity.
 - (5) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology was used to monitor Internet activity, including but not limited to social media accounts, the number of people affected, and what percentage of the reported monitoring was subject to (i) a warrant, and (ii) a non-warrant form of court authorization;
 - (6) Where applicable, a breakdown of what the surveillance technology was installed upon, including but not limited to on what vehicles or structures it was placed;
 - (7) Where applicable, a breakdown of what hardware surveillance technology software was installed upon;
 - (8) Where applicable, a breakdown of what databases the surveillance technology was aggregated in, including the frequency thereof;
 - (9) A summary of complaints or concerns that were received about the surveillance technology;
 - (10) The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;

Town of Cohasset
Sponsor Draft - Citizen Petition

- (11) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendment to the United States Constitution, the Massachusetts Constitution and all Massachusetts Laws and Regulations;
 - (12) Statistics and information about public records act requests, including response rates; and
 - (13) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.
- (b) Within thirty (30) days of submitting and publicly releasing an Annual Surveillance Report pursuant to Section 7 (a), the Covered Entity shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the Annual Surveillance Report and the Covered Entity's use of surveillance technologies.
- (c) Based upon information provided in the Annual Surveillance Report, the Select Board shall determine whether each surveillance technology identified in response to Section 7 (a), as used by the Covered Entity, has met the standard for approval and scope of authorization set forth in Section 5 (d) and 5 (e) of this by-law. If it has not, the Select Board shall direct the use of the surveillance technology be discontinued or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

SECTION 8. ENFORCEMENT AND REMEDIES

- (a) Any use of Surveillance Technology in violation of this by-law is declared unlawful and subject to enforcement as provided herein.
- (b) Any Covered Entity that violates this by-law shall be subject to:
- (1) An order to immediately cease use of the Surveillance Technology;
 - (2) An order to delete or destroy any Data and all associated metadata collected in violation of this by-law;
 - (3) Discipline in accordance with applicable personnel policies, collective bargaining agreements, and law;
 - (4) Such other remedies as may be available in law or equity.
- (c) This by-law may be enforced by the Town Manager, the Select Board, or the Town of Cohasset acting through Town Counsel, using any means available in law or equity. Before initiating any legal proceeding, the Town shall provide the Covered Entity with written notice of the alleged violation, and a period of not less than thirty (30) days within which to cure.

Town of Cohasset
Sponsor Draft - Citizen Petition

(d) Any resident of the Town of Cohasset shall have standing to bring a civil action in Superior Court to enforce the provisions of this by-law and to seek injunctive relief, declaratory relief, or other appropriate remedy.

(e) Any Town of Cohasset employee who reports, in good faith, an alleged violation of this by-law shall be entitled to the protections against retaliation set forth in M.G.L. c. 149 § 185 (Whistleblower Protection), subject to the limitations and requirements of that statute.

(f) Nothing in this section shall be construed to create individual civil liability for Town of Cohasset employees acting in good faith reliance on a facially valid authorization.

(g) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought to enforce this by-law.

SECTION 9. RELATIONSHIP TO STATE AND FEDERAL LAW

(a) This by-law is intended to supplement, and not supplant, applicable state and federal law, including but not limited to the Massachusetts Wiretap Statute, M.G.L. c. 272, § 99, and any applicable provisions of the Massachusetts data privacy laws or regulations.

(b) Nothing in this by-law shall be construed to prohibit the use of Surveillance Technology required by state or federal law or court order, or to limit law enforcement's use of Surveillance Technology pursuant to a valid warrant issued by a court of competent jurisdiction.

(c) If any provision of this by-law is held by a court of competent jurisdiction to be inconsistent with state or federal law, the remaining provisions shall continue in full force and effect.

(d) Nothing in this by-law shall be construed to: (i) transfer to Town Meeting or the Select Board any operational authority reserved to the Town Meeting by the Cohasset Town Manager Act or to the Police Chief by M.G.L. c. 41 § 97A; (ii) apply to Surveillance Technology owned and operated by a private property owner on that property owner's property, provided that such technology is not accessed, integrated, or used by the Town of Cohasset.

SECTION 10. RETROACTIVE COVERAGE FOR EXISTING SYSTEMS

Any Surveillance Technology in use or under contract by a Covered Entity as of the effective date of this by-law shall be required to submit the Disclosure Requirement in accordance with Section 5(c) to the Town Manager to submit to the Select Board within one hundred eighty (180) days of the effective date. A vote for approval by the Select Board as provided in Section 5, shall take place at the next scheduled Select Board meeting following the expiration of the second twenty (20) day period of public comment.

Town of Cohasset
Sponsor Draft - Citizen Petition

The Town Manager may request in writing a ninety (90) day extension for a particular Surveillance Technology, stating the reasons for the request, and the Select Board may grant a single extension for good cause.

If the Select Board does not approve a Surveillance Technology as provided in Section 5, the Covered Entity shall immediately suspend use of the Surveillance Technology until receipt of Select Board approval, or be considered in violation of the by-law and subject to Section 8 enforcement and remedies.

Nothing in this section shall be construed to require a unilateral breach of an existing contract. Where necessary, the Town Manager shall work with the Covered Entity, Vendor, and Town Counsel to bring the Surveillance Technology into compliance or to terminate the contract at the next available termination point consistent with the vendor agreement and M.G.L. c 30B.

This section does not apply to use within the Exigent Circumstances exception of Section 5(h).

SECTION 11. SEVERABILITY

If any provision of this by-law or the application thereof to any person or circumstance is held invalid by a court of competent jurisdiction, the remainder of the by-law and the application of its provisions to other persons or circumstances shall not be affected thereby.

SECTION 12. EFFECTIVE DATE AND APPROVAL

This by-law shall take effect thirty (30) days following its approval by the Attorney General of the Commonwealth pursuant to M.G.L. c. 40, § 32, and upon publication as required by law. The Select Board is directed to submit this by-law to the Attorney General for approval promptly following its passage at open town meeting.

SECTION 13. REVIEW

The Select Board, in consultation with the Town Counsel, shall review this by-law no less than every three (3) years and shall report to the open town meeting any recommended amendments to reflect changes in law, Surveillance Technology, or community standards.