1. ANNUAL SURVEILLANCE REPORT

Department:	**Emergency Communications**
Division or Unit (if applicable):	Emergency Communications Center
Submitted by:	Christina Giacobbe
Date:	2/28/2020
Surveillance Technology:	RapidSOS Emergency Data Integration System

1. **What Surveillance Technologies has the department used in the last year?**

   - RapidSOS Emergency Data Integration System (RapidSOS). RapidSOS is a web platform that provides life-saving data directly to 911 and first responders in an emergency, providing faster, more effective responses. In Cambridge, when callers contact 911 their call is directed to Emergency Communications on the state's Next Generation 911 platform and RapidSOS provides secondary, data-based location information to ECC through the RapidSOS clearinghouse. The purpose of this technology is to provide ECC Call Takers and Dispatchers with an accurate phone number and location information of wireless callers who contact 911 in our jurisdiction.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - The information obtained through this platform is not shared with any third party as the information is presented in real time. The department does share caller information and audio calls with the Police Department and District Attorney's Office as they proceed with prosecution. However, this information is provided through our 911 system, not RapidSOS.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - N/A

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- Yes. RapidSOS technology platform has been effective in proving location information during emergency calls for service. The RapidSOS platform continues to enhance capabilities in aiding in emergency responses.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - The department works with the City Solicitor's Office on all requests for caller information and audio calls. The department policy is that we do not release 911 calls, caller information or location information externally. The only exception is if the caller themselves requests the public record. The department shares caller information with law enforcement personnel who are authorized.

7. **What were the total annual costs of the Surveillance Technology?**

   - N/A. The department does not pay for any services related operating the State 911, Next Generation 911 system.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - The department does not know of any communities disproportionately impacted by RapidSOS as callers who contact 911 are doing so voluntarily to seek emergency services. When callers do contact 911, all calls are processed according to policy and protocol.

2. ANNUAL SURVEILLANCE REPORT

Department:	**Emergency Communications**
Division or Unit (if applicable):	Police
Submitted by:	Christina Giacobbe
Date:	2/28/2020
Surveillance Technology:	Trespass Tracking Database

1. **What Surveillance Technologies has the department used in the last year?**

   - Trespass Tracking Database. Information about no trespassing notices/letters provided to individuals who receive a no trespass order under Massachusetts law are recorded in the Trespass Tracking database. The Police Department is required to maintain these notices. All notices and the information in the notice are recorded in our Trespass Tracking database so that the information can be made readily available to first responders during calls for service.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - The information maintained in the Trespass Tracking is not shared with external parties. This information is shared with Cambridge Police to protect property and public safety and to hold those accountable who violate the orders.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - N/A

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - The Trespass Tracking database has been effective as it maintains up to date records of active Trespass Orders as well as safeguards those locations to increase public safety and quality of life.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

    - There have been no requests made to ECD for this information as it relates to the number of Trespass Orders or individuals in the database.

7. **What were the total annual costs of the Surveillance Technology?**

    - There is no cost for having the database as it is part of our Computer Aided Dispatch (CAD) platform.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

    - The department does not know of any communities that are disproportionately impacted by the Trespass Tracking database. Individuals are warned prior to being issued a no trespass order. The Police Department provides notice and will notify the ECC in the event a Trespass Order is issued so Emergency Communications can track it for them.

3. ANNUAL SURVEILLANCE REPORT

Department:	**Executive/City Manager**
Division or Unit (if applicable):	Public Information Office & Communications/Community Relations staff in: Arts Council, Community Development, Department of Human Service Programs, Library, Police Department, and Public Works
Submitted by:	Lee Gianetti
Date:	2/28/2020
Surveillance Technology:	• Media Monitoring - Meltwater • Social Media Monitoring - Meltwater Engage (Powered by Sprout Social):

1. **What Surveillance Technologies has the department used in the last year?**

    - **Media Monitoring - Meltwater**: Meltwater is a software as a service (SaaS) company that monitors media channels and social media platforms to identify relevant content based on keyword search terms. The platform provides access to a media influencers (media contacts) database, and is used to distribute city media releases. Meltwater is also used to monitor coverage of the City of Cambridge and key topic areas of interest (i.e. sustainability, construction, transportation, and Visionzero) to compile weekly reports to share with internal staff.

    - **Social Media Monitoring - Meltwater Engage (Powered by Sprout Social)**: Meltwater Engage is a software as a service (SaaS) that allows the City to coordinate the scheduling of social media posts, responding to messages, and evaluate the effectiveness of our social media efforts and strategy. Additionally, Meltwater Engage allows for direct connection to external help solutions (to open service request tickets) and provides a social customer relationship management (CRM) for staff within the platform.

2. **Has any Surveillance Technology data been shared with a third-party?**

    - No

3. **What complaints (if any) has your department received about Surveillance Technology?**

    - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

- N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **Media Monitoring** – **Meltwater**: This technology has allowed the City to respond to media reports regarding the City of Cambridge in a timely and appropriate manner and ensure the City's brand is appropriately represented. The platform allows us to measure the impact of our media outreach efforts and adjust strategy to improve coverage. The tool provides us with access to journalist and media outlet contacts from across the nation. The tool centralizes communication efforts that takes place by communications staff integrated throughout various city departments. It allows for centralized monitoring and coordination of citywide efforts.

- **Social Media Monitoring – Meltwater Engage**: This tool has allowed City departments to better coordinate social media efforts in terms of content reaction, strategy evaluation, and responsiveness to our followers. Not all departments have migrated into the tool yet but will in the coming years. The advantage of this tool is that all our social platforms can be accessed within one account, that is secured by various permission levels. It allows for quick access and control of City social media accounts during an emergency situation and provides a way for the city to coordinate the dissemination of information to the public.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- The Public Information Office did not directly receive any public records requests.

7. **What were the total annual costs of the Surveillance Technology?**

- **Meltwater** - $23,100 annual subscription cost from OOM from Public Information Office budget.
- **Meltwater Engage** - $33,500 annual subscription cost from OOM from Public Information Office budget.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- The Public Information Office is not aware of any.

4. ANNUAL SURVEILLANCE REPORT

Department:	**Finance**
Division or Unit (if applicable):	Assessing
Submitted by:	Gayle Willett
Date:	2/28/2020
Surveillance Technology:	Atlas RMV Portal

1. **What Surveillance Technologies has the department used in the last year?**

   - The Atlas RMV Portal. This is a web application provided by the Commonwealth of Massachusetts to access the RMV system. The RMV requires municipalities to use the ATLAS portal for accessing dealer plate information needed for excise tax billing. Assessing has limited access to this database and only uses it to create excise tax bills for billing car dealerships with dealer plates in Cambridge.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - No.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - None.

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. Assessing will continue to send out dealer plate excise tax bills.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - No.

7. **What were the total annual costs of the Surveillance Technology?**

   - All costs associated with Assessing's use for dealer plates billing are covered by the RMV.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - The department does not know of any communities disproportionately impacted by this technology. Please note that the technology is only used to search and verify information about car dealerships. The portal provides information that is not available to the public regarding the number of dealer plates at any dealership in Cambridge. The Assessing department has limited access to this database to three members of the department and has requested the least amount of information required for sending out dealer plate excise tax bills.

5. ANNUAL SURVEILLANCE REPORT

Department:	**Finance**
Division or Unit (if applicable):	Revenue
Submitted by:	Michele Kincaid
Date:	2/28/2020
Surveillance Technology:	Atlas RMV Portal

1. **What Surveillance Technologies has the department used in the last year?**

   - Atlas RMV Portal. This portal is used by three members of the Finance team to access the Commonwealth's RMV system. The portal allows staff to access a driver's information as reported on their driver's license, to administer the Motor Vehicle Excise Tax and release taxpayers from RMV Non-Renewal holds once their outstanding Motor Vehicle Excise Tax bill has been paid. The RMV Non-Renewal program assists the City in the collection of unpaid MVE taxes.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - No. The City does not share any data accessed through the Atlas RMV Portal with any other entity.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. The Registry Non-Renewal Surcharge program through the Atlas portal has been an effective tool in the City's collection process. For instance, the program attributed to the collection of 2,176 past due Motor Vehicle Excise Tax bills representing approximately $750,000 in FY19.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - No

7. **What were the total annual costs of the Surveillance Technology?**

   - The City is assessed an RMV fee on the annual Cherry Sheet Assessments. Massachusetts Statutes authorize an RMV surcharge of $20.00 per each clear transaction made through the Atlas RMV portal. The cost of the RMV surcharge is built into he fees incurred on late bills.
   - The City's assessments for 2019 & 2020 were:
     - 2019 – $423,400
     - 2020 – $461,860

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - The department is not aware of any community disproportionately impacted by this technology. An inquiry is only made through the portal if the taxpayer is paying a delinquent Motor Vehicle Excise tax bill that has been marked as Non-Renewal at the RMV. The taxpayer must pay their bill in cash or via credit card for the license hold to be released on this system.

6. ANNUAL SURVEILLANCE REPORT

Department:	**Information Technology**
Division or Unit (if applicable):	
Submitted by:	Mike Dugas, Eric Belford
Date:	2/28/20
Surveillance Technology:	IP Address Collection Platforms (Multiple)

1. **What Surveillance Technologies has the department used in the last year?**

   - IP Address Collection Platforms. The City of Cambridge uses various platforms that collect IP addresses from internal and external connections and connection attempts, e.g., the City website, Find It Cambridge, the City firewall and the City's web servers. While the platforms vary, the surveillance capabilities and functionality are the same. IP address information is used to limit and protect the City network from malicious sites and unauthorized access.

   - The city logs IP addresses on these technologies to aid in data protection, website performance and relevancy.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - No. This data is not shared with any third parties.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - No complaints have been received about IP collection.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A.

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. The City firewall and web servers, and the IP collection through the City's websites have been effective.
   - The Cambridge firewall is achieving its identified purpose. Currently we block:
     - about 1.5 Million overall events per day;
     - 100-200 critical events daily; and

    - 10-25 anti-bot events daily.
    - If the firewall misses a malicious IP, the logs on web servers are critical to diagnose site performance on a security perspective.
- The City of Cambridge collects information about visitors to public websites. This information has been leveraged to help better manage the sites. We have used this information to learn how many visitors we have, the websites they are coming from, which parts of our web site are of most interest to users and other facts that has helped us improve the web site and the services we offer.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- No.

7. **What were the total annual costs of the Surveillance Technology?**

- Firewall
    - $20,000 ongoing training
    - $50,000 annual maintenance

- Website(s)
    - Hosted on a Virtual Host which contains many servers, making a cost estimate difficult to pinpoint. Estimate $20,000 annual cost.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- No. The IP Address Collection Platforms, through the City's Firewall and Website(s), automatically operate in a standardized way. They impact all individuals attempting to access the City's websites in the same way.

7. ANNUAL SURVEILLANCE REPORT

Department:	**Law**
Division or Unit (if applicable):	
Submitted by:	Nancy Glowa
Date:	2/28/2020
Surveillance Technology:	WestLaw Public Records Search function

1. **What Surveillance Technologies has the department used in the last year?**

    - WestLaw Public Records Search function. This technology is used to gather publicly available information concerning litigants such as other lawsuits filed, judgments, convictions, warrants, bankruptcies, property records, and other publicly available filings or documents.

2. **Has any Surveillance Technology data been shared with a third-party?**

    - Yes, with the vendor WestLaw. The data is shared in circumstances where, due to technical difficulties with the software, the vendor rather than the attorney performs the search and provides the report.

3. **What complaints (if any) has your department received about Surveillance Technology?**

    - None.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

    - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

    - Yes.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

    - No.

7. **What were the total annual costs of the Surveillance Technology?**

- Unknown. The WestLaw subscription total cost is not broken down by feature.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- The department is not aware of any. This technology is only used in litigation on an as-needed basis to search public records for filings or documents concerning other litigants.

8. ANNUAL SURVEILLANCE REPORT

Department:	**Mayor's Office[1]**
Division or Unit (if applicable):	
Submitted by:	Wilford Durbin, Chief of Staff
Date:	2/28/2020
Surveillance Technology:	TweetDeck

1. **What Surveillance Technologies has the department used in the last year?**

- TweetDeck. Social media monitoring software/Twitter monitoring via TweetDeck. Used by Chief of Staff and Community Engagement and Communications Liaison to follow conversations on Twitter relevant to the Mayor's constituent services responsibilities, and to follow public discussion on matters before the Council. Current search criteria being compiled on TweetDeck for Mayor's Office use include the following: @Cambridge_Mayor, #CambMA, #Mapoli, @CambMA, +@CambMA.

2. **Has any Surveillance Technology data been shared with a third-party?**

- No.

3. **What complaints (if any) has your department received about Surveillance Technology?**

- None. In fact, the Mayor's Office usually hears the opposite—people who appreciate the Mayor responding to their constituent concern.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

- N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

[1] Marc McGovern served as Mayor of Cambridge in the 2018-2019 session. Mayor McGovern's Office used TweetDeck and submitted the first Annual Surveillance Report dated December 9, 2019. Current Mayor Sumbul Siddiqui did not use TweetDeck during the period covered by this Annual Surveillance Report. Because the technology was used during the reporting period, however, the City Manager is resubmitting this Annual Surveillance Report prepared by former Mayor Marc McGovern's Office.

- Quantifying the effectiveness of the use of TweetDeck by the Mayor's Office is admittedly difficult. Constituent concerns communications via Twitter have been used to generate policy orders to the City Manager, and Mayor's Office staff have transmitted information to Tweeter users, engaged in a public conversation, or otherwise interacted with a Tweet on a discretionary basis.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None.

7. **How much did it cost to acquire and operate Surveillance Technology?**

   - No costs associated with acquiring or operating TweetDeck. Office personnel may monitor TweetDeck data occasionally as part of their regular office duties.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - Impacts to privacy would likely not be felt by any individual, as a simple search of one's Twitter profile shows all Tweets, likes, retweets, and other activity from a user over the course of that profile's existence, and TweetDeck would not provide any additional information than could be found during such a search.

   - Twitter is the only social media platform that is regularly monitored by Mayor's Office staff, which means that those constituents who use other social media platforms do not have the same access to Office staff as Twitter users. Additionally, Twitter users are typically younger, more educated, and more likely to identify as Democrats than the general population. Twitter has been shown to be disproportionately popular among African American and Hispanic users.

   - The Mayor's Office has attempted to make itself available to a wider proportion of residents by hosting regular open office hours, employing a community engagement team, attending community events, and responding to communications that are received through mail, email, telephone, or other mediums.

9. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	Crime Analysis & CID
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	• Accurint Workstation • BRIC Omega Dashboard • Coplink • QED • Incident Database • CLEAR • LexisNexis • Focused Deterrence Database • LENS

1. **What Surveillance Technologies has the department used in the last year?**

- **Accurint Workstation**:
  - The Accurint Workstation is a software program utilized by CPD to analyze and map incident data from the Department's Incident Database, including arrest and incident reports; information contained in this database is gathered directly from QED, the Department's Records Management System (RMS).
  - The Department uses this software to produce daily, monthly and yearly maps; many that are disseminated publicly in various formats (Public Safety Bulletins, monthly Bridgestat, CPD Annual Crime Report, etc.).

- **BRIC Omega Dashboard**:
  - BRIC Omega Dashboard is the Intel portal for Boston Regional Intelligence Center (BRIC). The BRIC works at the forefront of intelligence collection and analysis. The BRIC allows for a regional approach to analyze whether crimes are interconnected by geography, type, or method. The BRIC covers the Metro Boston Homeland Security Region (MBHSR), consisting of: Boston, Brookline, Cambridge, Chelsea, Everett, Quincy, Revere, Somerville, Winthrop, The Greater Boston Police Council (Boston Area Police Emergency Radio Network—BAPERN), Massachusetts Bay Transportation Authority (MBTA), Massachusetts Port Authority (Massport), and Metro Fire Association.
  - In order to have the most complete accounting of what crimes and trends are impacting the region, it is necessary for all cities and towns, including Cambridge to contribute intelligence information. As such, the Cambridge Police Department contributes the following information: Approved arrest reports and Field

Interview and Observation (FIO) reports for certain cases (Confidential items, i.e., specifically marked domestic, juvenile, and sexual assault reports are excluded).

- **Coplink**:
    - COPLINK is one of the "solutions and services" provided through NESPIN (New England State Police Information Network®). COPLINK is a data sharing and crime analytics platform.
    - NESPIN (New England State Police Information Network®) is the local arm of a national project known as the RISS Program (Regional Information Sharing Systems). The goal of RISS is to assist local, state, federal and tribal Criminal Justice partners by providing adaptive solutions and services that facilitate information sharing, support criminal investigations, and promote officer safety. NESPIN is one of only six RISS centers operating nationwide.

- **QED**:
    - QED currently functions as CPD's Record Management System (RMS). A records management system (RMS) is "an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. In this context, records are limited to documents or electronic files directly related to law enforcement operations such as incident and accident reports, arrests, citations, warrants, case management, field contacts, etc."

- **Incident Database**:
    - The Incident Database is a Microsoft® Access database of corrected Records Management System Data. The database is used to "clean up" or to keep a more accurate record of the data that comes into the Records Management System (RMS) (i.e., initially an entry may be coded as a Larceny Motor Vehicle (L-MV) but through investigation it is determined to be a House Break where a L-MV also occurred—this database accurately reflects the appropriate Uniform Crime Reporting/National Incident-Based Reporting System code).

- **CLEAR**:
    - CLEAR® is a Public Records search engine. For a fee, CLEAR's database provides access to thousands of data sets including, address, phone numbers, billing (utilities, etc.) and credit-related information through public records and publicly available sources. According to its website:
        - "Thomson Reuters CLEAR® is powered by billions of data points and leverages cutting-edge public records technology to bring all key content together in a customizable dashboard. Locate hard-to-find information and quickly identify potential concerns associated with people and businesses

to determine if further analysis is needed. The user-friendly platform was designed with intuitive navigation and simple filtering parameters, so you can quickly search across thousands of data sets and get accurate results in less time."

  - In addition to accessing these public records to gather information on criminal suspects, the Department utilizes CLEAR to locate victims, witnesses and to verify background information on applicants (Public Safety Employment or License to Carry Firearms (LTC)).

- **LexisNexis**:
  - LexisNexis is a search engine. Users pay a fee to searchpublic records and other information compiled by the provider . It serves as a research tool used to locate people, companies, businesses, phone numbers, properties and fragments of information; this information helps to create a more complete picture of what we are investigating. (e.g., the Department entered the name and phone number of an individual who had been the victim of a scam, this search lead us to where the "scammer" found the victim's information, potentially creating a solid investigative lead).

- **Focused Deterrence Database**:
  - The Focused Deterrence Database uses an algorithm to analyze Records Management System (RMS) data based on past arrest and incident reports. The database algorithm identifies individuals who most recently have caused or been the subject of (i.e., victim/survivor) the greatest social harm and could currently benefit from social services and a case manager (offender or victim/survivor). CPD reaches out to individuals identified through the Database to offer them the option of joining the Focused Deterrence Program.
  - "Focused Deterrence" in terms of policing is a strategy that aims to deter specific criminal behavior through fear of specific sanctions, as well as anticipation of benefits for not engaging in crime. In its initial iteration here in Cambridge, Focused Deterrence closely resembled this. There have always been "variants" of the Focused Deterrence program in practice; here in Cambridge, Focused Deterrence has morphed into an altogether different program.
  - Focused Deterrence in Cambridge does not utilize a predictive policing program, through the Focused Deterrence Database or otherwise. The department does not have a "gang database" (or any semblance thereof) and instead pulls information directly from the CPD RMS.

- **LENS (Law Enforcement Notification System)**:
  - The Law Enforcement Notification System (LENS) is a web-based system which provides local law enforcement with information on federal offenders currently on supervision with the U.S. Courts. This release of information is required by the

Violent Crime Control Act of 1994**.** Qualifying offenders include those convicted of certain drug trafficking crimes, crimes of violence, sex offenses and those convicted of internet child pornography offenses included as part of the Sex Offender Registration and Notification Act. LENS allows real time updates regarding these offenders and provides the ability to search neighboring jurisdictions and nationwide.

2. **Has any Surveillance Technology data been shared with a third-party?**

    - **Accurint Workstation**: No. But the Department uses this software to produce daily, monthly and yearly maps; many that are disseminated publicly in various formats (Public Safety Bulletins, monthly Bridgestat, CPD Annual Crime Report, etc.).
    - **BRIC Omega Dashboard**: Yes. The Department shares incident data with the BRIC on a daily basis for effective regional law enforcement.
    - **Coplink**: Yes. The Department shares incident data with Coplink on a daily basis for effective statewide law enforcement.
    - **QED**: Yes. The Department regularly shares incident data with fellow law enforcement and provides records for public records requests.
    - **Incident Database**: Yes. The Crime Analysis Unit creates weekly, monthly and annual reports based on this crime data.
    - **For all other technologies**: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

    - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

    - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **Accurint Workstation**:
    - Yes, the technology has been effective in realizing the stated purpose. This technology allows the Crime Analysis Unit to effectively analyze and map crime, which is an essential function of a modern police department.

- **BRIC Omega Dashboard**:

    - Yes, the technology has been effective in realizing the stated purpose. The technology allows the Department to obtain regional crime data (and crime mapping) about local offenders/offenses on a daily basis to help effectively solve crime and make arrests.

- **Coplink**:
    - Yes, the technology has been effective in realizing the stated purpose. The technology allows the Department to obtain statewide crime data (and crime mapping) about local offenders/offenses on a daily basis to help effectively solve crime, make arrests and licensing decisions.

- **QED**:
    - Yes, the technology has been effective in realizing the stated purpose. QED serves as the central report writing and incident documentation system for the Department. The Department is required by state and federal law, as well as court procedural rules to document a variety of police encounters, whether for criminal, civil or administrative matters.

- **Incident Database**:
    - Yes, the technology has been effective in realizing the stated purpose. This database is a condensed accounting of QED incidents for purposes of crime incident statistical reporting. This database is effectively utilized for weekly, monthly and annual crime reporting.

- **CLEAR**:
    - Yes, the technology has been effective in realizing the stated purpose. The technology allows Department personnel to effectively search public records and publicly available records to locate offenders, victims and witnesses for criminal investigations and trials. This database is also an effective tool for licensing decisions.

- **LexisNexis**:
    - Yes, the technology has been effective in realizing the stated purpose. The technology allows Department personnel to effectively search public records and publicly available records to locate offenders, victims and witnesses for criminal investigations and trials. This database is also an effective tool for licensing decisions.

- **Focused Deterrence Database**:

  - Yes, the technology has been effective in realizing the stated purpose. The technology allows the Department to analyze criminal data and objectively identify those individuals who are causing the greatest amount of social harm to the community and/or are in need of social services. The database has not been utilized since the last Annual Surveillance Report was submitted.

- **LENS**:
  - Yes, the technology has been effective in realizing the stated purpose. The technology allows the Department to identify Cambridge residents who are on federal probation.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- None

7. **What were the total annual costs of the Surveillance Technology?**

- **Accurint Workstation**:
  - $30,000 per year; previously budgeted through "E-Gov" but will be included in the police budget beginning FY'21.

- **BRIC Omega Dashboard**:
  - The BRIC Omega Dashboard has no financial costs to the City of Cambridge. It is funded by the Department of Homeland Security.

- **Coplink**:
  - RISS/NESPIN/COPLINK has no financial costs to the City of Cambridge. It is funded by the federal government. The actual cost is unknown at this time.

- **QED**:
  - QED is a longstanding multi-agency product (Police, Fire, ECD). Its initial costs are unknown. According the Director of ECD the combined annual maintenance cost for all three agencies is $60K.

- **Incident Database**:
  - This database is created using Microsoft® Access, available through the City's Microsoft Office suite, and is of little to no cost to the Department.

- **CLEAR**:

    - CPD currently has access to 5 licenses furnished to the Department by the Urban Area Security Initiative (UASI) at no cost to the agency. Information as to actual cost was not furnished by UASI.

- **LexisNexis**:
    - Included in Accurint Workstation costs.

- **Focused Deterrence Database**:
    - There is no cost associated with this technology; two CPD Detectives are assigned to this program in addition to their other duties/responsibilities.

- **LENS**:
    - There are no costs to CPD, the program is federally managed and funded.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **Accurint Workstation**:

    - The department is not aware of any community disproportionately impacted by this technology. This technology has a minimal impact as the software analyzes incident data already stored in the Department's records management system. The Department is required by state and federal law, as well as court procedural rules to document a variety of police encounters, whether for criminal, civil or administrative matters.

- **BRIC Omega Dashboard**:

    - The department is not aware of any community disproportionately impacted by this technology. However, anytime that large amounts of intelligence information are gathered, significant privacy implications exist. The BRIC maintains a strict policy designed to "protect individual privacy, civil rights, civil liberties, and other protected interests" [Boston Regional Intelligence Center Privacy, Civil Rights and Civil Liberties Protection Policy].

        - The 43-page policy states [in part]: The BRIC will not seek or retain and originating agencies will agree to not submit information about individuals or organizations solely 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 orientation.

    - The Cambridge Police are committed to responsibly accessing regional systems in manners that are consistent with Cambridge values and in compliance with its ordinances and practices. Based on its current usage and the significant safeguards in place, this technology has a minimal privacy impact on Cantabrigians and surrounding communities.

- **Coplink**:
  - The department is not aware of any community disproportionately impacted by this technology. The NESPIN/RISS Centers operate their intelligence system under the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations [CFR] Part 23). All RISS member agencies have agreed to comply with the requirements of 28 CFR Part 23 with respect to any criminal information they submit into an applicable RISS Criminal Intelligence Database (RISS/Intel). RISS has adopted a comprehensive privacy policy to protect individual privacy, civil rights, civil liberties, and other protected interests [RISS's Commitment to Safeguarding Privacy, Civil Rights, and Civil Liberties].
  - The Cambridge Police Department is committed to responsibly accessing regional systems in manners that are consistent with Cambridge values and in compliance with its ordinances and practices.
- **QED**:
  - The department is not aware of any community disproportionately impacted by this technology. QED serves as the central report writing and incident documentation system for the Department. The Department is required by state and federal law, as well as court procedural rules to document a variety of police encounters, whether for criminal, civil or administrative matters.
  - The Cambridge Police Department is committed to responsibly maintaining systems in manners that are consistent with Cambridge values and in compliance with its ordinances and practices. Only CJIS Compliant Certified Public Safety Employees in the performance of their official duties may access, use or disseminate information contained in QED for official and lawful criminal justice purposes. Based on its current usage and the significant safeguards in place, this technology has a minimal privacy impact on Cantabrigians and surrounding communities.
- **Incident Database**:
  - The department is not aware of any community disproportionately impacted by this technology. This database is a condensed and corrected accounting of QED incidents for purposes of crime incident statistical reporting. The Department is required by state and federal law, as well as court procedural rules to document a variety of police encounters, whether for criminal, civil or administrative matters.
  - The Cambridge Police Department is committed to responsibly maintaining systems in manners that are consistent with Cambridge values and in compliance with its ordinances and practices. Only CJIS Compliant Certified Public Safety

Employees in the performance of their official duties may access, use or disseminate information contained in this “limited” database for official and lawful criminal justice purposes. Based on its current usage and the significant safeguards in place, this technology has a minimal privacy impact on Cantabrigians and surrounding communities.

- **CLEAR**:
  - The department is not aware of any community disproportionately impacted by this technology. Thomson Reuters’ CLEAR boast providing access to “billions of data points and thousands of datasets”. Thompson Reuters is a private, for-profit company that provides its service for a fee. The Cambridge Police Department is committed to responsibly accessing this service in a manner that is consistent with Cambridge’s values. The likelihood of disparately impacting a particular population via using this technology is small, as it has broad uses, aimed at providing information to assist the Department in providing services for those who have been harmed and locating those who have caused the harm.
- **LexisNexis**:
  - The department is not aware of any community disproportionately impacted by this technology. LexisNexis is a private, for-profit company that provides its service for a fee. The Cambridge Police Department is committed to responsibly accessing this service in a manner that is consistent with Cambridge’s values.
- **Focused Deterrence Database**:
  - The department is not aware of any community disproportionately impacted by this technology. This technology has a minimal impact as it analyzes existing incident reports from the Department’s RMS. The Department is required by state and federal law, as well as court procedural rules to document a variety of police encounters, whether for criminal, civil or administrative matters. The algorithm utilizes factors such as “role” played and “when” the incident occurred (allowing for a decaying weighted analysis). Additionally, crimes are weighted in strict accordance with Massachusetts Sentencing Guidelines.
  - The Department is committed to responsibly utilizing data in a way that is protective of privacy, civil rights and civil liberties. Currently 6 individuals are in the Focused Deterrence program. As a point of reference, the Focused Deterrence database was not utilized for the 2019/2020 Focused Deterrence firearms violence program. Involved parties were identified through RMS arrest and firearms incident reports from the previous three years.
- **LENS**:
  - The department is not aware of any community disproportionately impacted by this technology. This technology has a minimal impact as the Department only

has access to information about those individuals who are Cambridge residents that are on federal probation. The information is accessed via restricted web site for official use only, and provided through federally managed application/portal. Only CJIS Compliant Certified Public Safety Employees in the performance of their official duties may access, use or disseminate information contained in LENS for official and lawful criminal justice purposes. The LENS web site informs users that "…Unauthorized use is subject to prosecution under Title 18 of the U.S. Code", and that "…all activities and access attempts are logged"

10. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	CID Days, DV/SA & Cyber
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	• GPS tracking devices (2) • Digital Intelligence Workstation • Dell Laptop BCERT • Magnet Forensics–Axiom • Getdata Forensic Explorer • Shotspotter

1. **What Surveillance Technologies has the department used in the last year?**

- **GPS Tracking Devices**:
  - Global Positioning System (GPS) is a technology that makes possible exact location tracking through satellite trilateration using a network of satellites orbiting the Earth. The satellites are able to communicate with specialized receivers on the ground, providing the exact location of the receiver.
  - The CPD possess and utilizes two of these receivers to assist in certain criminal investigations (thefts of bicycles and packages). A GPS device is attached to a bicycle or package that might be stolen and, if a theft occurs, CPD tracks the item.

- <u>Cell phone and computer forensic analysis tools</u>:
  - **Digital Intelligence Workstation**:
    - Digital Intelligence Workstation is one of many tools utilized by the Criminal Investigation's Cybercrime Unit to investigate computer-related crimes. This hardware allows Cybercrime Detectives to "image" a hard-drive for future analysis by computer software tools (Axiom-Magnet Forensics and/or Getdata Forensic Explorer).
  - **Dell Laptop BCERT**:
    - Dell Laptop BCERT is hardware that is utilized to recover evidence from computer equipment (hard-drives, etc.).
  - **Magnet Forensics – Axiom**:
    - Axiom-Magnet Forensics is software that can analyze the history of a file, recover digital evidence and analyze and report on digital evidence.
  - **Getdata Forensic Explorer**:
    - Getdata Forensic Explorer is software that can analyze digital evidence by locating, filtering, sorting and keyword searching.

- **Shotspotter**:
    - Shotspotter is a gunshot detection system deployed across the City, which listens for gunshots over a 1.1 square mile coverage area in the City. Gunshot detection systems are designed to be an ever-vigilant reporting ear. CPD has no listening capabilities; sensors are analyzed at Shotspotter HQ in California. Only incidents identified by Shotspotter's proprietary algorithm as "in the class of gunshots" generate a numerical address sent to the Department via the application. No other audio is sent to or sought by CPD.

2. **Has any Surveillance Technology data been shared with a third-party?**

- **Shotspotter**:
    - Yes. Members of the Metro Boston UASI region can receive Cambridge Shotspotter notifications for officer and public safety.
- **For all other technologies**: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

- None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

- N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **GPS Tracking Devices**:
    - Yes, the technology has been effective in realizing the stated purpose. The technology has allowed the Department to identify a number of bike and package thefts.

- <u>Cell phone and computer forensic analysis tools</u>:
    - **Digital Intelligence Workstation**; **Dell Laptop BCERT**; **Magnet Forensics – Axiom**; and **Getdata Forensic Explorer**:
        - Yes, the technology has been effective in realizing the stated purpose. The technology has allowed detectives from the Department's Cyber Unit to effectively search and analyze computers and cell phones in dozens of criminal investigations.

- **Shotspotter**:
    - Yes, the technology has been effective in realizing the stated purpose. The technology has effectively detected gunshot activity and allowed officers to more efficently repond to relevant crime scense. The evidence derived from this technology has also been utlilzed in several criminal proescutions.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- **Shotspotter**: Yes. Three requests.
    1. Requestor was looking for gun fire data generated by Shotspotter. The Department provided relevant CAD data.
    2. Requestor was looking for records on live fire testing for Shotspotter, which were provided.
    3. Requestor was looking general information about Shotspotter and the accuracy of the technology. The Department provided relevant CAD reports and gunshot data for the requested timeframe.

- **Other technologies**: No.

7. **What were the total annual costs of the Surveillance Technology?**

- **GPS Tracking Devices**:
    - None.

- <u>Cell phone and computer forensic analysis tools</u>:
    - **Digital Intelligence Workstation**; **Dell Laptop BCERT**; **Magnet Forensics – Axiom**; and **Getdata Forensic Explorer**:
        - None

- **Shotspotter**:
    - Approx. $50K /yr., which is funded by the Urban Area Security Initiative (UASI).

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **GPS Tracking Devices**:
    - The department is not aware of any community disproportionately impacted by this technology. While the privacy implications for tracking individuals and items using GPS are wide-ranging; the technology as currently employed by the Cambridge Police Department should have no disproportionate impact because it

is only utilized to track property (bikes/packages) stolen from the Cambridge Police Department.

- Cell phone and computer forensic analysis tools:
    - **Digital Intelligence Workstation**; **Dell Laptop BCERT**; **Magnet Forensics – Axiom**; and **Getdata Forensic Explorer**:
        - The department is not aware of any community disproportionately impacted by this technology. Where police engage in a search of any type, privacy concerns are at their highest. This technology is utilized in a wide berth of investigations in which a cell phone or computer device is lawfully seized. The technology is only utilized where there is no reasonable expectation of privacy, after consent is provided or a search warrant is obtained.

- **Shotspotter**:
    - Individuals who live, work or are otherwise located within the geographic area of its microphones/sensors may be impacted by the technology. The placement of microphones has not changed since the implementation of the technology. Initial placement was based on prevalence of gunfire or gunshot victims. CPD can request movement but the high concentration (relative to Cambridge) has persisted in the same area.

11. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	SIU
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	• Covert Cameras (Keltech Covert Streetlight Camera, CSA Pole Camera, IVC Covert Camera) • DTC Body Wire

1. **What Surveillance Technologies has the department used in the last year?**

   - **Covert Cameras**:
     - Covert cameras are deployed only in serious cases that pose a significant security or public safety risk. Cameras are placed in specified locations to capture images of suspected illegal activity. Per policy, these cameras cannot be deployed without the approval of a Police Superintendent or the Police Commissioner.

   - **DTC Body Wire**:
     - Body wire is an audio surveillance device and is only used for officer safety purposes during undercover operations (controlled drug buys, prostitution stings, human trafficking, etc.). An officer wears the body wire to record audio of their surroundings.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - **For all technologies**: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **Covert Cameras**: Yes, the technology has been effective in realizing the stated purpose. The cameras were effectively deployed in the past to surveil public locations that were hotspots for firearm activity.

- **Body Wire**: Yes, the technology has been effective for officer safety during undercover drug and vice operations.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- None

7. **What were the total annual costs of the Surveillance Technology?**

- **Covert Cameras**: None.
- **Body Wire**: None.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **Covert Cameras**:
    - This technology captures images of a discreet location. This technology was deployed last year in public places in communities where there was a documented pattern of firearms activity. Deployment of this technology occurred with Command Staff level approval after a demonstrated risk to public safety.
    - This technology has minimal impact as it is typically used for brief periods in public spaces that do not implicate constitutional protections.
    - This technology is only used in constitutionally protected spaces with consent, a search warrant or exigent circumstances.
        - Note: This technology has been/is used in protected spaces during investigations with third-party consent: (e.g., complainant thought that the presence of dead animals on multiple occasions may have been some type of threat; permission was given for CPD to place covert camera in protected space to capture image of culprit; it was determined that the dead animals were being placed by another animal).
- **Body Wire**: The department is not aware of any community disproportionately impacted by the technology. Body wires are deployed during undercover drug and vice operations for officer safety.

12. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	Crime Scene Services, Booking & Records
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	• Morpho Automated Fingerprint Identification System (AFIS) with camera (Massachusetts State Police (MSP) System) • Live Scan (3 devices)

1. **What Surveillance Technologies has the department used in the last year?**

- **Morpho AFIS**:
  - Morpho is a fingerprint database through the Massachusetts State Police. It allows the Department's Crime Scene Serves Section to compare unknown latent fingerprints to a state database of known fingerprints when investigating criminal activity.

- **Live Scan**:
  - Digital fingerprint system with live feed to the Massachusetts State Police and Federal Bureau of Information for identification and criminal history. Live Scan is used to document and identify persons in lawful police custody or those persons who voluntarily wish to be fingerprinted. The technology is also utilized for statutorily mandated background checks for firearms licensing and to comply with federal and state security requirements for City employees

2. **Has any Surveillance Technology data been shared with a third-party?**

- **Morpho AFIS**:
  - For each case where this technology is utilized, data is shared with the MSP. If a latent print is individualized to a known print by members of the Department's Crime Scene Services Unit, the data will be shared with an external police department for verification purposes under the ACE-V methodology for fingerprint analysis.

- **Live Scan**:
  - Every live scan procedure is shared with the FBI and MSP. The FBI shares fingerprints with other federal agencies, including the Department of Homeland Security.

- For all technologies: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - **Morpho AFIS**:
     - Yes. The technology has been effective in realizing the stated purpose. The technology has allowed the Department to identify a number of offenders based on latent fingerprints left at crime scenes or on evidence.

   - **Live Scan**:
     - Yes. The technology has been effective in realizing the stated purpose. The technology allows the Department to verify the identity of someone in police custody and obtain their federal and state criminal history for law enforcement purposes. The technology is also effective for completing firearms licensing background checks and security requirements for City employees.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None

7. **What were the total annual costs of the Surveillance Technology?**

   - **Morpho AFIS**: Annual maintenance costs are $4,571.

   - **Live Scan**: Annual maintenance costs are $9,660.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **Morpho AFIS**:
  - The department is not aware of any community disproportionately impacted by this technology. It is utilized to analyze all unknown latent fingerprints recovered from a crime scene or evidence.
- **Live Scan**:
  - The department is not aware of any community disproportionately impacted by this technology. This technology is used to document and identify all persons in lawful police custody. This technology is also utilized for all persons voluntarily seeking to be fingerprinted, voluntarily applying for a license to carry a firearm, or who voluntarily seek unattended access to the police station.

13. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	EOD
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	• Wireless Explosive Ordinance Disposal (EOD) robots with cameras: Robotex Avatar II 2 (3); Foster Miller Tallon 4; Foster Miller Dragon Runner 4; Remotetec F6A 4 with fiberoptic • Tactical Electronics VF52 Fiber Scope • ATF Bomb Arson Tracking System (BATS)

1. **What Surveillance Technologies has the department used in the last year?**

- **Wireless EOD robots with cameras**:
  - These devices provide robot gripper and camera assistance that can be remotely deployed to provide a live image of a suspected explosive device. The devices are various sizes: Robotex Avatar II 2 is a small platform, Foster Miller Tallon 4 & Foster Miller Dragon Runner 4 are medium platform, and the Remotetec F6A 4 with fiberoptic is a large platform.
  - These devices provide fast and reliable threat assessment for explosive ordinance disposal and bomb technicians. Grippers allow for device manipulation. Cameras allow for visual inspection via distance.

- **Tactical Electronics VF52 Fiber Scope**:
  - Optical scope technology used to view enclosed or secure areas for explosive mitigation.
  - Provides fast and reliable threat assessment for EOD and bomb technicians.

- **ATF BATS**:
  - The Bomb Arson Tracking System (BATS) is a web-based case management system that allows state and local arson and explosive investigators access to up-to-date arson and explosive data from across the nation.

2. **Has any Surveillance Technology data been shared with a third-party?**

- **Wireless EOD robots with cameras** and **Tactical Electronics VF52 Fiber Scope**:
  - No. The EOD does not use this technology to record any data.
- **ATF BATS**:

    - Yes. The Department enters bomb and arson cases into this system, which are shared with the federal Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

3. **What complaints (if any) has your department received about Surveillance Technology?**

- None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

- N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **Wireless EOD robots with cameras** and **Tactical Electronics VF52 Fiber Scope**:
    - Yes. The technology has been effective in realizing the stated purpose. This technology has been regularly deployed to determine whether explosive devices are in a given location or piece of property.

- **ATF BATS**:
    - Yes. The technology has been effective in realizing the stated purpose. The technology allows the Department's EOD to report and track arson and bomb cases.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- None

7. **What were the total annual costs of the Surveillance Technology?**

- **Wireless EOD robots with cameras**:
    - None.
- **Tactical Electronics VF52 Fiber Scope**:
    - None.
- **ATF BATS**:
    - None. Access provided by ATF at no charge.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **Wireless EOD robots with cameras** and **Tactical Electronics VF52 Fiber Scope**:
    - The department is not aware of any community disproportionately impacted by this technology. This technology is utilized minimally during exigent circumstances when an explosive device is believed to be present. The images captured are only of the suspected explosive device and its immediate surroundings.
- **ATF BATS**:
    - The department is not aware of any community disproportionately impacted by this technology. This technology is only used to track arson and bomb incidents.

14. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	Fleet
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	Prisoner Transport Security Cameras (Transport Wagon 236 & 240)

1. **What Surveillance Technologies has the department used in the last year?**

   - Prisoner Transport Security Cameras. Prisoner Transport Security Cameras provide enhanced safety for transporting officers and prisoners by recording the circumstances of individuals' transportation by CPD.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - For all technologies: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. The technology has been effective in realizing the stated purpose. The cameras are used to view persons lawfully in police custody who are being transported by the Department and are effectively used for their safety and the safety of the transporting officers.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- None

7. **What were the total annual costs of the Surveillance Technology?**

- None

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- The department is not aware of any community disproportionately impacted by this technology. This technology is only used to view persons lawfully in police custody who are being transported by the Department and is implemented strictly for their safety and the safety of the transporting officers. The information is saved for 14 days and is automatically written over unless affirmative action is taken to save a particular piece of footage.

15. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	SRT
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	Throwbot XT

1. **What Surveillance Technologies has the department used in the last year?**

   - Throwbot XT. This technology is a throwable micro-robot platform that enables operators to obtain instantaneous video and audio. The device does not record. It can be placed, or made to travel (crawl), into hazardous situations (without risking human exposure to harm) in order to allow operators to quickly make informed decisions when seconds count.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - None

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - The technology has been effective in realizing the stated purpose. This technology has allowed the Special Response Team to assess whether a threat exists before making lawful entry or taking further action.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None

7. What were the total annual costs of the Surveillance Technology?

- The most recent maintenance cost was $1,750.

8. Are any communities disproportionately impacted by Surveillance Technology?

- The department does not know of any community disproportionately impacted by this technology. This technology is used in minimal situations where an exigency exists and the Special Response Team needs to assess whether a threat exists before making lawful entry or taking further action. The audio and video captured in real time are not recorded or stored.

16. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	CID
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	Case Cracker

1. **What Surveillance Technologies has the department used in the last year?**

   - Case Cracker. Case Cracker is a video recording technology used in interview rooms at the police stations to document police interviews.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - For all technologies: The Department provides the Middlesex District Attorney's Office with mandatory discovery on all criminal prosecutions.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. The technology has been effective in realizing the stated purpose. The technology effectively records interviews in the Criminal Investigations Division.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None

7. **What were the total annual costs of the Surveillance Technology?**

- None.

8. Are any communities disproportionately impacted by Surveillance Technology?

- The department is not aware of any community disproportionately impacted by this technology. Recordings are all done voluntarily. Audiovisual recordings are posited to alleviate public concerns connected with suspect treatment in custodial settings. There is a compelling societal interest in requiring video recording of police interviews and interrogations. The benefits of recording custodial interrogations go above and beyond transparency. The benefits extend not only to the accused, but also to the police, defense attorneys, prosecutors, fact finders, and the public.[1]

[1] Bang, B. et al. (2018) Police Recording of Custodial Interrogations: A State-by-State Legal Inquiry.

17. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	Professional Standards
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	Infraware

1. **What Surveillance Technologies has the department used in the last year?**

   - Infraware. Infraware is dictation software that records a person's voice for transcription purposes.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - No. This technology is utilized for internal investigations through the Department's Professional Standards Unit.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes. The technology has been effective in realizing the stated purpose. This technology has allowed the PSU to obtain transcripts for internal investigations.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None

7. **What were the total annual costs of the Surveillance Technology?**

- None

8. Are any communities disproportionately impacted by Surveillance Technology?

- No. This technology is utilized to obtain transcripts of voluntary interviews given during internal PSU investigations.

18. ANNUAL SURVEILLANCE REPORT

Department:	**Police**
Division or Unit (if applicable):	PIO
Submitted by:	Commissioner Branville Bard & Jim Mulcahy
Date:	2/28/2020
Surveillance Technology:	TweetDeck

1. **What Surveillance Technologies has the department used in the last year?**

   - TweetDeck. TweetDeck is a social media dashboard application for management of Twitter accounts. Originally an independent app, TweetDeck was subsequently acquired by Twitter Inc. and integrated into Twitter's interface. TweetDeck allows users to organize and search Tweets in various ways.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - None, other than the actual posting of social media on Twitter.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes, the technology has been effective in realizing the stated purpose. This technology has allowed the PIO to view Twitter mentions and posts about the Department.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - None

7. **What were the total annual costs of the Surveillance Technology?**

- None. TweetDeck is a free application in Twitter.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- The department is not aware of any community disproportionately impacted by this technology. Of course, TweetDeck only gathers data from individuals who use Twitter. However, this technology has a minimal impact as the software merely aggregates publicly available Twitter posts and mentions about the Department.

19. ANNUAL SURVEILLANCE REPORT

Department:	**Public Health**
Division or Unit (if applicable):	Public Health Nursing Epidemiology and Data Services
Submitted by:	Claude Jacob
Date:	2/28/2020
Surveillance Technology:	MAVEN (Massachusetts Virtual Epidemiologic Network)

1. **What Surveillance Technologies has the department used in the last year?**

   - MAVEN (Massachusetts Virtual Epidemiologic Network). MAVEN is a PHIN (Public Health Information Network) compliant, secure web-based surveillance and case management system for infectious diseases that enables rapid, efficient communication among local and state health departments and laboratories. MAVEN allows the department to conduct case investigations and management.

2. **Has any Surveillance Technology data been shared with a third-party?**

   - Surveillance data is only shared with the Massachusetts Department of Public Health, as required by state law.

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - MAVEN remains an essential tool for CPHD to complete state-mandated infectious disease investigation work. For example, in 2018, CPHD received reports of 873 reportable infectious diseases among Cambridge residents; of these, 148 required follow-up and investigation by public health nursing and epidemiology staff.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- No public records requests were received.

7. **What were the total annual costs of the Surveillance Technology?**

- Costs for the acquisition, operation, and maintenance of MAVEN are covered by the Massachusetts Department of Public Health. CPHD staff use MAVEN to do state-mandated infectious disease investigations but are not involved in maintenance of the system.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- All confirmed and suspected cases of reportable infectious diseases among Cambridge residents are required to be reported to the state health department and/or the Cambridge Public Health Department through MAVEN, where they are managed and investigated. Representation in the MAVEN system is a function of the distribution of disease in the Cambridge population and the health care utilization rates among Cambridge residents, both of which may vary by sub-group within Cambridge. Wherever possible, CPHD considers the potential over- or under-representation of marginalized communities in Cambridge in our infectious disease investigation work.

20. ANNUAL SURVEILLANCE REPORT

Department:	**Cambridge Public Schools**
Division or Unit (if applicable):	Information, Communications & Technology Services
Submitted by:	James Maloney
Date:	2/28/2020
Surveillance Technology:	Securly for Chromebooks Web Filter

1. What Surveillance Technologies has the department used in the last year?

- Securly for Chromebooks Web Filter. This technology is employed as a web filter only on all CPS Chromebooks. The filter is a Chrome plugin that is managed and deployed at the Google Domain level to all CPS owned Chromebooks. One this is setup it requires no other maintenance. The web filter will block sites that are considered potentially unsafe or harmful to students.

- Securly blocks the following categories of content: Pornography, Drugs, Gambling, Other Adult Content, Social Media, Anonymous Proxies, Chat Messaging, Hate, Social Networking, Streaming Media and Games. There is also a Keyword blocking as well. These are "Generic" filter settings established by Securly.

2. Has any Surveillance Technology data been shared with a third-party?

- No. All vendor provided-applications employed by the school department that may, or do, collect student-level data are protected against inappropriate use of student data by the vendor through Student Data Privacy Agreements (DPA). These agreements ensure that any and all student-level data collected is only used for the purpose of providing the service the vendor was engaged for, and nothing else. All school department DPAs are available on the CPS website.[1] The DPAs employed by CPS are both a MA State and National Model DPA developed by the Student Data Privacy Consortium[2] and leveraged throughout the K12 Educational Technology Marketplace to protect student data from inappropriate uses.

3. What complaints (if any) has your department received about Surveillance Technology?

[1] See https://sdpc.a4l.org/district_listing.php?districtID=457

[2] See https://privacy.a4l.org/

- One complaint was received by students at CRLS. This complaint was on the filtering functionality – questioning the algorithm behind what content was being filtered or not. As a result of this complaint a new CRLS committee has been formed that will be providing input and guidance on content filter settings for high school students.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes, all student issued Chromebooks are filtered as required by the Children's Internet Protection Act (CIPA).

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - No

7. **What were the total annual costs of the Surveillance Technology?**

   - N/A. CPS employs the free version of Securly.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - All students utilizing CPS issued Chromebooks at home are receiving the same level of content filtering. Students that have access to personal or family devices to complete required student work at home are not bound by the same filter that is intended to protect students from potentially harmful content.

21. ANNUAL SURVEILLANCE REPORT

Department:	**Cambridge Public Schools**
Division or Unit (if applicable):	Safety & Security, Transportation
Submitted by:	James Maloney
Date:	2/28/2020
Surveillance Technology:	• Bus Video Recorders • GPS Devices • Edulog Transportation System

1. **What Surveillance Technologies has the department used in the last year?**

- **Bus video recorders**: Cameras are installed on all school buses. The cameras on the school buses allow the school department to review any incidents that take place, after the event is over. The cameras allow the department to determine the source of any behavioral issues on the bus. The footage helps CPS staff and parents clarify what actually happened during an incident and supplements any report from a student or bus driver.

- **GPS devices**: These devices are installed on vehicles transporting sudents. GPS units are attached to the student transportation vehicles to monitor and report back the physical location of the vehicles to the CPS Transportation Department. The GPS units monitor the physical location of each vehicle in real time.

- **Edulog Transportation System**: The Edulog Transportation system is a database used by the CPS Transportation Department to manage the bus routes and student assignments. All information about what buses students ride as well as the buses locations are stored and managed within this system.

2. **Has any Surveillance Technology data been shared with a third-party?**

- **Bus video recorders**: Yes, but in limited circumstances. In some cases, parents can view the video footage generated by the video recorders, but parents can only view footage of their child.

- **GPS devices**: Yes. GPS location data is shared with the contracted transportation company to aid in the delivery of the bus transportation service. Parents can also view data on the location of the bus to which their child is assigned through a secure parent portal.

- **Edulog Transportation System**: Yes. Data on bus routes and locations is shared with the contracted transportation company to aid in the delivery of the bus transportation service. Parents can also view data on the route of the bus to which their child is assigned through a secure parent portal.

3. **What complaints (if any) has your department received about Surveillance Technology?**

- **Bus video recorders**: None.

- **GPS devices**: The only complaints received were from parents of students riding the busses when the "parent portal" was not accurately reflecting the bus arrival times due to an error of some sort.

- **Edulog Transportation System**: None.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

- N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **Bus video recorders**: Yes. While the number of disciplinary incidents requiring investigation varies annually, videos are used in approximately 30 to 60 investigations each year.

- **GPS devices**: Yes. Parents have been informed of bus arrival times.

- **Edulog Transportation System**: Yes. The system successfully built and tracked bus routes and student assignments.

6. **Did the department receive any public records requests concerning Surveillance Technology?**

- No.

7. **What were the total annual costs of the Surveillance Technology?**

- **Bus video recorders**: No costs in the past year.

- **GPS devices**:
  - Ongoing Maintenance – $1,579/year
  - Source of Funds – School General Fund

- **Edulog Transportation System**:
  - Ongoing Maintenance – $19,660/year
  - Source of Funds – School General Fund

8. Are any communities disproportionately impacted by Surveillance Technology?

- CPS is not aware of any communities disproportionately impacted by these technologies.

22. ANNUAL SURVEILLANCE REPORT

Department:	**Traffic, Parking, and Transportation**
Division or Unit (if applicable):	**Parking Management, Street Management**
Submitted by:	Joe Barr, Brooke McKenna, Stephanie McAuliffe
Date:	2/28/20
Surveillance Technology:	• ATLAS RMV Portal (Parking Management) • Traffic Signal Detection Cameras (Street Management Division) • MioVision Traffic Count Mobile Camera Units (Street Management Division)

1. **What Surveillance Technologies has the department used in the last year?**

- **ATLAS RMV Portal**: ATLAS is a web application provided by the Commonwealth of Massachusetts to access the RMV system and used by the Parking Management division. It used by Parking Services staff to issue resident parking permits, view handicap placard information, and clear holds on licenses and vehicle registrations. No data is collected or stored, and the public cannot access it.

- **Traffic Signal Detection Cameras**: These cameras are deployed at a limited number of signalized intersections across the City. The detection cameras include 360-degree units manufactured by MioVision and directional cameras manufactured by Iteris. They are used for detection of roadway users, to classify their mode of transportation, and to quantify their movements at signalized intersections in the City of Cambridge, and to assist in the optimized operation of traffic signals. The aggregated data collected will be analyzed and used to improve the efficiency and safety of operations for all roadway users. The technology will also provide City staff with continuous roadway user counts to allow for evaluation of seasonal and annual traffic volume variations to assist in future design and planning projects.

- **MioVision Traffic Count Mobile Camera Units**: These units are deployed in the field by transportation consultants, at various locations on a temporary basis. The units are typically attached to a signal, utility, or streetlight pole within the right of way. This technology collects traffic video and data that is later processed to provide a variety of traffic related data such as turning movement counts, intersection counts and classifications, and road volume counts. Additionally, there is an optional "Connect" component that can be added to Scout units that allows the unit to communicate wirelessly for monitoring purposes (but not to stream data) and has the capability of detecting MAC addresses from devices searching for wireless networks within their range. With the added ‘Connect” functionality, the Scout Unit can detect devices within an 80-100 foot radius of the unit. The Scout Unit uses MD5 hash function to produce a 128 bit hash value for each MAC address, pseudonymizing the MAC addresses. This process is unidirectional and cannot be reversed, but the MAC addresses remain unique and matchable. These hashed addresses and timestamps are stored in the unit during the data collection period then transmitted to a central system operated by the vendor, MioVision. The central system then looks to see if the same hashed MAC address has been recorded previously by other scout units in the vicinity and in the same time frame and uses any matches to establish travel times.

2. **Has any Surveillance Technology data been shared with a third-party?**

- **ATLAS**: No data has been shared with a third-party.

- **MioVision Intersection Cameras**: These cameras are accessed by the Vendor, MioVision, for purposes of set up, training, and troubleshooting of the product.

- **MioVision Traffic Count Mobile Camera Units**: Video from these units is collected and accessed by Transportation Consultants. Given that past deployment has taken place without City approvals, we cannot determine who has accessed the data. Moving forward, a permitting system will allow us to understand who is collecting data.

3. **What complaints (if any) has your department received about Surveillance Technology?**

- **ATLAS**: None

- **MioVision Intersection Cameras** and **MioVision Traffic Count Mobile Camera Units**: The department has received inquiries about the installed cameras from time to time, but no inquiries that the department would characterize as complaints. We explain the use of the technology and that has been satisfactory for individuals inquiring. Moving forward, we will formally log all incoming inquiries about the technologies.

4. **Were any violations of the Surveillance Use Policy found in the last year?**

    - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

- **ATLAS**: Yes. ATLAS is used daily by Parking Services staff to issue resident parking permits, view handicap placard information and clear license and registration holds. In 2019, 38,381 Resident Parking Permits were issued. In FY19, there were 17,973 chargeable clears for license and registrations holds.

- **Traffic Signal Detection Cameras**: The MioVision units were installed in late 2019 and are functioning as expected. We will be better able to assess the success of the units once we have collected enough data to use for analysis. The directional cameras operate as expected and detect vehicles in order to optimize signal operations.

- **MioVision Traffic Count Mobile Camera Units**: Yes. These data collection units are a significant improvement over past manual and tube data collection methods. In the past, counts have been taken by hand, which is far more labor intensive and limits the amount and timeframe of the data collected. Tubes used for data collection frequently malfunctioned or were destroyed by road traffic or street cleaning vehicles. Overall, the video-based data collection allows for better data collection, and as a result, far better data analysis for transportation planning. In addition, it is becoming increasingly difficult to obtain detailed counts using any other methodology as most vendors are using this technology.

6. Did the department receive any public records requests concerning Surveillance Technology?

- In January, the department received a request from John Hawkinson that was sent to via email to the City Manager's office. He requested records that answered the following questions about the **Traffic Signal Detection Cameras** at Ames/Main Street:

  1. Make/model number of the cameras?
  2. How many are deployed?
  3. Where are they installed?
  4. Date of installation and activation?
  5. Whether the fact that they do not record is enforced by configuration, by software, by hardware, or some other mechanism?
  6. Effect on bicycles and non-auto vehicles?
  7. Effect on cycle times?

  The Public Records Access Officer responded with a sales brochure about the cameras and the signal plans for the Ames and Main Street intersection.

- In late March we received a request via an email to the Public Records Access Officer for all records related to the City's pilot programs with MioVision and Draper. The requestor did not provide any more details about what they were looking to learn. The Public

Records Access Officer provided all records except for emails. One document was withheld as it was exempt from disclosure because the document related to policy positions being developed by the City. A total of 10 records were provided.

- In total, we've received two requests, both of which came via email, and provided 12 records.

7. **What were the total annual costs of the Surveillance Technology?**

- **ATLAS**: There is a $20.00 RMV surcharge for license plate clears. In FY 2019, there were 17,973 chargeable clears for license and registrations holds, which are assessed through a reduction in local aid provided on the Cherry Sheet Assessments.

- **Traffic Signal Detection Cameras**: The cameras were acquired for $166,000, funded by Casino Mitigation Funds.

- **MioVision Traffic Count Mobile Camera Units**: N/A. These are typically installed by traffic engineering consultants as part of the overall cost of a transportation planning or traffic engineering study, such as a Traffic Impact Study required for a private development project.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

- **ATLAS**: The Portal allows TPT staff to access detailed personal information about Cambridge residents. The information accessed is not collected or stored and the public cannot access it. The information is only accessed by Parking Services staff when issuing resident parking permits, viewing handicap placard information, and clearing holds on licenses and vehicle registrations, all of which are requested by the customer. The data available on the Portal may have a greater impact on the privacy of those individuals who own a vehicle than those individuals who do not own a vehicle, since staff only access the vehicle registration data for residents who own cars. Access to the Portal is password protected and the Parking Services Staff who use ATLAS receive individual, detailed training which includes best practices for protecting personal information. As such, the use of the Massachusetts RMV Website Portal does not have any disproportionate impact on any population.

- **Traffic Signal Detection Cameras**: Although they are installed in specific communities that have specific demographics, they observe all users that pass through an intersection, whether or not those users come from those local communities. Typically, these units are installed at major intersections which carry both local and regional traffic. The technology does not retain any personally identifiable information, and does not impact the drivers, cyclists and pedestrians that are counted by the cameras. As such, the use of Detection Cameras does not have any disproportionate impact on any one population.

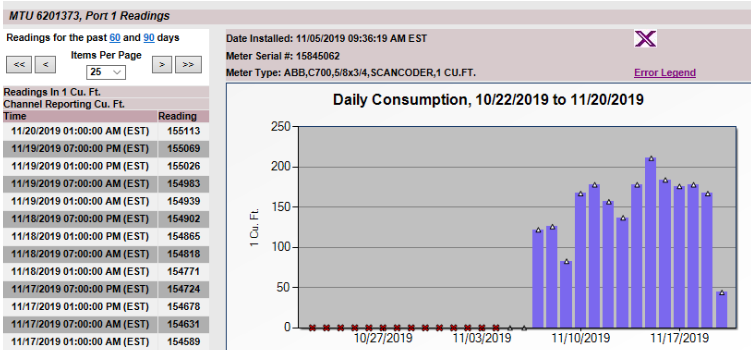
- **MioVision Traffic Count Mobile Camera Units**: The units record all users that pass by the unit, whether or not those users come from those local communities. These units are also deployed for very short periods of time, further limiting impacts. While data collection is used across the City, it is possible that data collection, and thus video recording, will occur most frequently in areas with significant new development, thus possibly impacting these areas more than parts of the City with less development. However, these cameras primarily collect data that is not personally identifiable and use hashing technology to mask MAC addresses that could otherwise be personally identifiable. Overall, the use of MioVision Intersection Cameras does not have disproportionate impacts on any population.

23. ANNUAL SURVEILLANCE REPORT

Department:	**Water**
Division or Unit (if applicable):	
Submitted by:	Sam Corda & Fred Centanni
Date:	2/28/2020
Surveillance Technology:	Automated Meter Reading (AMR) System

1. What Surveillance Technologies has the department used in the last year?

- Automated Meter Reading (AMR) System. The Water Department's AMR system is a radio-based system which transmits on a Federal Communication Commission (FCC) licensed/reserved frequency. Meter Transmitter Units (MTUs) are attached to every water meter throughout the city. The MTU transmits water meter reads in a propriety format. These reads are transmitted every 4 hours on a floating schedule. For example, an MTU will transmit a read today at 6:00AM, and then transmit a read tomorrow at 6:03AM. The reads are received by the Data Collection Units (DCUs) located within the city. The DCUs transmit the meter readings, using a cell phone network, to a communications computer located at the Water Department. The communications computer then transfers the data to a database computer which translates the data in order for the city to view the water meter reads. This allows the Water Department to provide actual reads for billing and allows us to alert customers for potential leaks at their property. Below is an example of our STAR AMR software and the data collected:



MTU 6201373, Port 1 Readings

Readings for the past 60 and 90 days

Items Per Page 25

Readings In 1 Cu. Ft.
Channel Reporting Cu. Ft.

Time	Reading
11/20/2019 01:00:00 AM (EST)	155113
11/19/2019 07:00:00 PM (EST)	155069
11/19/2019 01:00:00 PM (EST)	155026
11/19/2019 07:00:00 AM (EST)	154983
11/19/2019 01:00:00 AM (EST)	154939
11/18/2019 07:00:00 PM (EST)	154902
11/18/2019 01:00:00 PM (EST)	154865
11/18/2019 07:00:00 AM (EST)	154818
11/18/2019 01:00:00 AM (EST)	154771
11/17/2019 07:00:00 PM (EST)	154724
11/17/2019 01:00:00 PM (EST)	154678
11/17/2019 07:00:00 AM (EST)	154631
11/17/2019 01:00:00 AM (EST)	154589

Date Installed: 11/05/2019 09:36:19 AM EST
Meter Serial #: 15845062
Meter Type: ABB,C700,5/8x3/4,SCANCODER,1 CU.FT.

2. Has any Surveillance Technology data been shared with a third-party?

- No

3. **What complaints (if any) has your department received about Surveillance Technology?**

   - None

4. **Were any violations of the Surveillance Use Policy found in the last year?**

   - N/A

5. **Has Surveillance Technology been effective in achieving its identified purpose?**

   - Yes

6. **Did the department receive any public records requests concerning Surveillance Technology?**

   - No

7. **What were the total annual costs of the Surveillance Technology?**

   - The department is nearing completion of an upgrade of the AMR system to replace all the MTUs because the batteries reached their life expectancy. $177,490.00 was spent on installation in the last year.
   - The department also has a contract to upgrade the DCUs and software for $48,380.
   - **Ongoing maintenance** – The department has an annual maintenance agreement for approximately $15,000.
   - **Source of funds** – Capital Water Funds for upgrade; Operating Water Funds for the annual maintenance agreement.

8. **Are any communities disproportionately impacted by Surveillance Technology?**

   - No. Every property that has a water service has a water meter regardless of any other criteria. This allows CWD to provide actual reads for billing and to alert all customers of any potential leaks in their property