



BROOKLINE POLICE DEPARTMENT

Office of Professional Responsibility

ANDREW LIPSON
CHIEF OF POLICE

LT. PAUL R. CAMPBELL
Office of Professional Responsibility

To: Chief Andrew Lipson

From: Lieutenant Paul Campbell

Date: December 3, 2018

Subject: CIMS Audit

Sir:

Pursuant to Special Order 2010-4 III(c)(3), I conducted an audit of the Brookline Police Department Critical Infrastructure Monitoring System. The CIMS policy requires that the Office of Professional Responsibility conduct a semi-annual audit to determine compliance with this policy and also to ensure that CIMS records are complete and up to date.

The CIMS system consists of 11 cameras set up in various locations throughout the Town of Brookline. The policy requires training of police officers and dispatchers prior to receiving codes to access the system. The policy also requires records be kept regarding use of the system as well as requests for production of captured video. Additionally, a camera inventory log must be maintained documenting that the cameras are inspected monthly. As part of the camera inventory logs the location of the cameras as well as dates placed in service are recorded.

The CIMS camera policy calls for the cameras to operate every day between the hours of 10 PM – 6 AM. During those hours the cameras are to be automatically turned on via computer. From 6 AM until 10 PM, the same computer is supposed to close a “privacy ensuring cap” (called Situcon covers) over the cameras, effectively taking them offline. During 2015, the CIMS cameras reached their end of life, and the decision was made to replace the cameras. The new cameras would not work with the Situcon covers that had been in place with the original cameras. Efforts to locate “privacy ensuring caps” for the new cameras were not successful, and as a result the cameras are not covered during the off hours of the policy (6 AM – 10 PM). Additionally, for the past several audits (since June of 2015) the camera at Boylston/Hammond has been out of service for Wi-Fi network



issues. This has now been addressed and as of September 2018 that camera is back up and running. At the present time all 11 CIMS cameras are up and running. All of the cameras operate without covers, and as such all cameras operate 24 hours a day. This has been the case since 2015, and been reported in numerous prior audits.

I have confirmed with the Technology Division that video recordings are retained for 14 days, at which point the recordings are overwritten. We have operated on this schedule since CIMS was implemented. My reading of the law is that we are likely in violation of the Municipal Retention Schedule for digital recordings, which should be held for 1 month (Municipal Records Retention Schedule - Schedule number 01.007 – “Audio/Visual tape or Digital Recordings, security and surveillance tapes – retain 1 month”). I would suggest we consider retaining the video for 30 days as opposed to the current 14 day schedule. Special Order 2010-4 Section V provides for this, specifically stating that CIMS recordings are to be retained for fourteen days “unless otherwise required by the evidence policy, by court order, or by law.” Officer Scott Wilder has told me that we currently have the storage space to retain the video for 30 days, so if we were to change this it would require no hardware upgrades. It simply requires a change to the scheduling in the software. As I believe we are currently in violation of the law, I recommend this change be implemented.

Video Recording Production Requests

The Technology Division maintains a log documenting each request made for a copy of a video captured by the CIMS cameras. Requests for video are submitted to Officer Scott Wilder, who retains a hard copy of each request. Additionally he logs data associated with the request, including date/time of incident, type of incident, location, case # if applicable, date request filled and any additional remarks to explain the nature of the request.

I inspected this log and determined it to be organized and up to date. Since July 1, 2018 there have been 18 requests for production of video captured by the CIMS camera system. 17 of these video requests were made by law enforcement personnel for law enforcement reasons, while 1 request was a public records request. The sole public records request was related to a motor vehicle crash, however this could not be filled as the camera did not capture the incident.

Of the 18 total requests for video, 10 were actually accommodated. The remaining requests were not filled because the cameras did not record any video of value.

Below is a list of the CIMS camera video requests for this audit period.

Date of Incident	Time of Incident	Type of Incident	Turned Over To
7/8/2018	1630 hrs	stolen bait bike	N/A – camera pointing in the wrong direction
7/10/2018	0135 hrs	Investigation	Evidence
7/11/2018	1845 hrs	MV Crash	Evidence



7/25/2018	1545 hrs	Larceny of scooter	Evidence
8/12/2018	0430 hrs	Indecent A&B	N/A – camera not in position to view incident
8/13/2018	1033 hrs	Larceny	N/A – Not in view of camera
8/16/2018	1312 hrs	MV crash 3 vehicles	Computer room evidence
8/13/2018	0649 hrs	MV crash	Computer Room Evidence
8/16/2018	0500 hrs	A&B	Detective Lacy
8/19/2018	1215 hrs	MV Crash	N/A – Not in view of camera
8/19/2018	1215 hrs	MV Crash	N/A Public Records Request – Not in view of camera
9/1/2018	0755 hrs	MV Crash	N/A – Not in view of camera
9/17/2018	0530-0545 hrs	Hit & Run Bicycle	Computer Room Evidence
10/7/2018	0315 hrs	OUIL	Evidence
10/10/2018	0020 hrs	stolen motorcycle	Evidence
10/17/2018	1010 hrs	Pedestrian Struck	Evidence
10/29/2018	2140 hrs	Indecent A&B	N/A – Not in view of camera
11/19/2018	1205 hrs	Runaway	N/A – Not in view of camera

Camera Inventory and Inspection

Under the policy it is required that the camera system be inspected monthly by the Technology Division. Additionally the Technology Division must maintain a log inventorying all cameras in service, including the date each camera is placed in service, location, inspection dates, maintenance/repair history and specific activities being monitored if any.

The log detailing this information is kept in the Larimore property system. A separate log is maintained for each camera. The information contained in the logs is complete and easily accessible. I checked the logs and found the information to be clear and up to date. The



cameras have been inspected as required. Where issues were discovered they were noted in the inspections as well as the repairs undertaken to correct these issues.

Certification/Training

Prior to receiving an access code to operate the CIMS camera system, Department Employees are required to receive a copy of the policy for the CIMS cameras. Employees must also receive training in the policy, with a focus on impermissible uses. Once this is done, employees then sign a certification that they have received and read the Special Order regarding the CIMS camera system (S.O. 2010-4).

This certification/training component of the Special Order is being adhered to. Department personnel have all been provided a copy of the policy. Additionally, the policy is available to all department personnel at any time via the department's online file storage system. The entire department was trained in the camera system and impermissible uses at the time the cameras were installed. CIMS policy training is provided to new hires prior to their being provided an access code to the system. Signed certifications are maintained within the training division. A training notebook with all certifications was readily available, and as new employees are hired their certifications are added to the notebook for review. I verified that the newest dispatchers have all been trained, and confirmed that they have signed certifications documenting that they have received training pursuant to SO 2010-4. Within the last 3 months we have hired 16 new police Officers. All of these new officers have been trained as well. These officers have signed the same certifications which have also been added to the training notebook.

Complaints/Misuse

There have been no complaints, either internal or external related to use of the CIMS camera system. Since the inception of the CIMS network, there has never been an allegation of impermissible use of any of the equipment.

Conclusion

Based on my audit the cameras are being used lawfully and for appropriate purposes. The camera records are being maintained and are up to date and organized. Officers are being educated on the policy regarding the use and impermissible uses of the CIMS camera system, and after reviewing these policies they sign a certificate acknowledging they have been trained regarding the CIMS camera system. These training records are being properly maintained and updated. The CIMS camera system is not in compliance with the CIMS policy regarding the privacy ensuring caps, which is something that is well-known. The cameras record 24 hours a day. This fact has been reported in my previous audits, has been discussed by the Brookline Select Board at their meetings, and has also been reported in the Brookline Tab. We do not use the Situcon covers any longer and have not used them in several years. At the current time the policy still includes language regarding the physical covering of the cameras. This language in the policy is outdated and at some



point should be removed. Aside from this issue, the CIMS cameras are otherwise being operated in compliance with Special Order 2010-4.

Respectfully submitted,

A handwritten signature in blue ink that reads "LT Paul Campbell" with a stylized flourish at the end.

Lieutenant Paul Campbell
Office of Professional Responsibility

