

Implementation of the Security Video Surveillance Policy

Date:	March 5, 2008
To:	Government Management Committee
From:	Chief Corporate Officer
Wards:	All
Reference Number:	P:\2008\Internal Services\F&re\Gm09026F&re - (AFS 8718)

SUMMARY

This report describes the implementation of the Toronto Video Surveillance Policy from Council adoption of the Policy in July 2006 to present and highlights the priority implementation areas for 2009.

Financial Impact

There are no new financial requirements emanating from this report.

DECISION HISTORY

At its September 17, 2008 meeting, the Government Management Committee approved a staff report, "Security Video Surveillance Update Report", from the Chief Corporate Officer that provided a two-year review of the Security Video Surveillance Policy.

At its meeting of October 21, 2008, the Government Management Committee reopened the staff report and requested "...that the Chief Corporate Officer, in consultation with the Director, Corporate Access and Privacy (CAP), report back to the Government Management Committee for its meeting on January 14, 2009, on the implementation of the Toronto Video Surveillance Policy in accordance with the provisions of the Policy adopted in July 2006.

ISSUE BACKGROUND

In July 2006, City Council approved the City of Toronto Security Video Surveillance Policy (the Policy). This policy addresses key requirements of the *Municipal Freedom of Information and Protection of Privacy Act* and provides guidelines and protocols governing video surveillance including:

- a) the designation of the Chief Corporate Officer of the City of Toronto as the responsible executive for the Security Video Surveillance Policy;
- b) identifying roles and responsibilities for personnel responsible for policy implementation and governance, as well as, individuals using and maintaining CCTV equipment;
- c) identifying factors to be considered prior to implementing video surveillance including: factors to consider prior to using cameras, considerations when designing and installing video surveillance equipment, providing notice of the use of video surveillance through posted signs, designating who and under what conditions personnel are authorized to operate camera equipment, and providing obligations to personnel who have access to records;
- d) addressing issues related to the collection, use, disclosure, retention and destruction of recordings in accordance with the privacy requirements of MFIPPA and its Regulations;
- e) detailing procedures to facilitate access to records, including formal access requests and access for law enforcement purposes; and,
- f) providing a review clause indicating that the policy will be reviewed every two years by the Chief Corporate Officer who will forward recommendations for update, if any, to City Council for approval;

At its meeting of July 2006, City Council further added that a protocol be developed by the Chief Corporate Officer, in consultation with Union representatives, to discuss and provide notice to Union representatives of the removal or addition of security video surveillance cameras.

COMMENTS

Implementation of the Security Video Surveillance Policy

To date, the major focus of the implementation of the Security Video Surveillance Policy has been directed toward six priority areas:

1. *Posting the applicable video surveillance “Notice of Collection” sign*

These signs had to be posted at all entrances, and/or prominently displayed on the perimeter of the grounds, at all City facilities that use security video surveillance equipment. This sign can be found in “Appendix #3 – Notice of Collection” of the Security Video Surveillance Policy.

2. *Conducting Security Video Threat Assessments prior to all new installations*

Before deciding to install video surveillance, a number of factors must be considered such as:

- a) The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- b) A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- c) An assessment must be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated.
- d) The proposed design and operation of the video surveillance systems should minimize privacy intrusion.

In response to security incidents or threats, a recognized security threat assessment process is followed to assist in determining the applicable security measure(s) to be specified. A security video camera is only one of many measures that can be specified and only after other measures have been considered and rejected as unworkable.

Following the adopted Policy, each security camera installed since July 2006 has had an assessment conducted prior to the installation following the form found in “Appendix 5 - Surveillance Video Security Threat Assessment” of the Policy. A copy of each assessment is delivered to the Corporate Access and Privacy Office and a copy is also provided to CUPE Local 79 where they have members who work from or attend that City site.

3. Securing access to all security video system recorders

As detailed in the policy, all reception/recording equipment and records must be stored securely in a locked receptacle located in an access-controlled area. Each location with a video surveillance recording device had to be verified for Policy compliance and the applicable, locked recording device receptacle had to be installed at sites that were not compliant.

4. Training all persons designated as Operators and having them sign the “Security Video Surveillance Policy Training Checklist”

Operators are City staff or contracted individuals entrusted by Corporate Security or a Designated Divisional Management staff member to operate the video surveillance system for a particular facility. To ensure these Operators are aware of all obligations under the Security Video Surveillance Policy, a “Security Video Surveillance Policy Training Checklist” was provided as Appendix 6 of the Security Video Surveillance Policy. To date all Security Officers have completed and signed the Training Checklist.

5. Development of a Notice Protocol

City Council requested a protocol be developed by the Chief Corporate Officer, in consultation with Union representatives, to discuss and provide notice to Union representatives of the removal or addition of security video surveillance cameras. The Human Resources Division has led this initiative of the development of a Notice Protocol. A draft protocol has been prepared and is awaiting sign off by CUPE Local 79.

6. Ensuring systems / cameras are repaired and maintained in functioning order

In order to comply with the Security Video Surveillance Policy, all security video equipment must be actively working and must be appropriately maintained. Upon adoption of the policy a number of security video surveillance systems had components which were not functioning. All security video systems are now functioning.

2009 Security Video Surveillance Work plan

For 2009, the major focus of the implementation of the Security Video Surveillance Policy is being directed toward three new priority areas:

1. Conducting Security Video Threat Assessments for installs completed prior to 2006

While Security Video Threat Assessments have been completed for all installations since the adoption of the Policy by City Council, in order to comply with the fundamental vision of the Policy, assessments still must be completed for security video installations completed prior to July 2006. These assessments form a significant amount of work as comprehensive security assessments must be completed prior to even reviewing the sites video components to ensure the most applicable security measures were installed and that

other measures of deterrence or detection have been considered and rejected as unworkable. Corporate Security has initiated this review process and will anticipate completion prior to the next reporting out period.

2. Training

The Security Video Surveillance Policy provides obligations on a number of staff to provide or attend training regarding the Policy. This privacy training will be developed by the Corporate Access and Privacy Office and will be administered to applicable City and contract staff as detailed in the Policy and will act as a compliment to Appendix #6 of the Policy, "Video Surveillance Policy Checklist".

3. Policy Audit

The Information & Privacy Commissioner of Ontario (IPC) has recommended that high profile CCTV installation programs be audited for policy compliance by a third party using the GAPP Privacy Framework. Following the IPC's recommendations, the Corporate Security Unit will undertake to engage a suitable third party auditor to perform a policy compliance audit of the Security Video Surveillance Policy as part of their 2009 workplan.

CONCLUSION

The next information report will include recommendations on changes to the retention schedule, the inclusion of the protocol to discuss and provide notice to the Union representatives of the removal or addition of security video surveillance cameras, and the inclusion of a procedure for requesting video that is not covered under the statutory obligations of the *Municipal Freedom of Information and Protection of Privacy Act*.

CONTACT

Mike McCoy
Director, Facilities Operations
(Tel) 416-397-5270
(Fax) 416-392-4828
mmccoy@toronto.ca

Dwaine Nichol
Manager, Security & Life Safety
(Tel) 416-397-7129
(Fax) 416-397-5403
dnichol@toronto.ca

SIGNATURE

Bruce Bowes, P. Eng.,
Chief Corporate Officer