TORONTO

AUDITOR GENERAL'S REPORT ACTION REQUIRED
with Confidential Attachment

Facilities Management – Security and Safety Improvements Required

Date:	February 3, 2015
To:	Audit Committee
From:	Auditor General
Wards:	All
Reason for Confidential Information:	This report involves the security of property belonging to the City or one of its agencies and corporations.
Reference Number:	

SUMMARY

The Auditor General's Audit Work Plan included a review of Facilities Management – Security and Safety. Corporate Security provides security services at over 1,300 City facilities including City Hall, Metro Hall, civic centres, Union Station and divisional facilities. The objective of this audit was to assess the adequacy and effectiveness of the physical security and safety measures at City facilities.

Our audit findings and recommendations are detailed in Appendix1 to this report. Some of the report sections pertaining to the security of property that belongs to the City contain confidential information. These audit findings are presented separately to this report in confidential Attachment 1.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the Chief Corporate Officer to develop a plan to complete a review of physical security at all City facilities using a risk based approach and to address any deficiencies found during the review.

2. City Council request the Chief Corporate Officer to perform the appropriate follow up reviews to ensure identified security deficiencies are adequately addressed by the divisions.

3. City Council request the Chief Corporate Officer to update Site Information Packages after significant changes have been made to a facility and periodically for all facilities.

4. City Council request the Chief Corporate Officer to implement a process to ensure that all closed circuit television cameras not on the network are regularly checked and equipment deficiencies for all equipment are documented and repaired.

5. City Council adopt the recommendation contained in Confidential Attachment 1 to this report.

6. City Council request the Chief Corporate Officer to regularly obtain employee termination reports from Corporate Human Resources and upon review cancel user access as required.

7. City Council request the Chief Corporate Officer to run reports to identify inactive access cards and upon review, cancel user access as required.

8. City Council request the Chief Corporate Officer to implement a review process for corporate sites to identify terminated access cardholders and remove access in accordance with security policies.

9. City Council request the Chief Corporate Officer ensure that all access card request forms have the necessary information, access requirements and approvals completed before processing.

10. City Council request the Chief Corporate Officer to review the current level of mobile patrolling activity to determine if it adequately meets requirements and propose options for the actions, if any, necessary to satisfy the security needs.

11. City Council request the Chief Corporate Officer to update run sheets and develop a protocol to ensure that all City facilities are patrolled over a reasonable period of time by using a combination of scheduled and random patrols.

12. City Council request the Chief Corporate Officer to ensure that supervisors periodically run a status report for open incident reports and close them in a timely manner once resolved.

13. City Council request the Chief Corporate Officer to periodically review work orders for the vendors responsible for the maintenance of security equipment that have been outstanding for longer than two weeks and to follow-up with the vendor to resolve outstanding deficiencies in a timely manner.

14. City Council request the Chief Corporate Officer to request monthly reports and supporting documentation from the vendor and to review and monitor performance. When deficiencies are identified, appropriate corrective action should be taken.

15. City Council request the Chief Corporate Officer to review all time and material invoices billed since July 1, 2014 by the vendor and initiate recovery of any overpayments.

16. City Council request the Chief Corporate Officer to ensure that payments for services are not made to vendors until all work has been completed according to the contract specifications.

17. City Council request the Chief Corporate Officer to further develop and implement performance measures that will promote performance improvement, effectiveness, efficiency, and appropriate levels of internal controls.

18. City Council request the Chief Corporate Officer to review the current requirement for use of force training and make any necessary adjustments to corporate requirements.

19. City Council request the Chief Corporate Officer to store all corporate training records for security guards in a centrally maintained database, to update training records in a timely manner and to monitor compliance with training requirements.

20. City Council request the Chief Corporate Officer to ensure that emergency plans are tested by conducting drills or exercises for important portions of the plan and that the results be reviewed and changes be made to the plan accordingly.

21. City Council request the Chief Corporate Officer to periodically update policies and procedures to reflect current operational practices, improvements to safety and security, and after any significant changes in processes or security incidents.

22. City Council not authorize the public release of the confidential report in Attachment 1 as this report involves the security of property belonging to the City or one of its agencies and corporations.

Financial Impact

The recommendations in this report have no financial impact.

COMMENTS

Overall, we found that physical security and safety measures at City facilities need improvement. The implementation of the recommendations in our report will improve security and safety at City facilities. Key issues were identified in the following areas:

- Physical security
- Access cards

- Mobile Unit operations
- Administrative processes

The Auditor General's report entitled "Facilities Management – Security and Safety Improvements Required" is attached as Appendix 1. Management's response to all the recommendations contained in the report, except confidential recommendation number 5, is attached as Appendix 2.

This report also includes a confidential Attachment 1 that relates to the security of property that belongs to the City.

CONTACT

Jerry Shaubel, Director, Auditor General's Office
Tel: 416-392-8462, Fax: 416-392-3754, E-mail: jshaubel@toronto.ca

Gawah Mark, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8439, Fax: 416-392-3754, E-mail: gmark@toronto.ca

SIGNATURE

_____
Beverly Romeo-Beehler, Auditor General

14-FMS-01

ATTACHMENTS

Attachment 1: Confidential Information
Facilities Management – Security and Safety Improvements Required

Appendix 1: Facilities Management – Security and Safety Improvements Required

Appendix 2: Management's Response to the Auditor General's report Facilities Management – Security and Safety Improvements Required

AUDITOR GENERAL'S REPORT

Facilities Management – Security and Safety Improvements Required

February 3, 2015

Beverly Romeo-Beehler, CPA, CMA, B.B.A., JD
Auditor General

TORONTO

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Auditor General's Audit Work Plan included a review of Facilities Management – Security and Safety. Corporate Security provides security services at over 1,300 City facilities. This includes City Hall, Metro Hall, civic centres, Union Station and divisional facilities.

Audit Objective

The objective of this audit was to assess the adequacy and effectiveness of the physical security and safety measures at City facilities.

Physical security and safety measures should be strengthened

Overall, we found that physical security and safety measures at City facilities needs improvement. Security deficiencies of various kinds were noted at all 10 facilities we audited.

Improvements are required in key areas, including: security patrols, access cards and clearing incidents that have been outstanding for a long time in the system. Confidential Attachment 1 contains additional findings that involve the security of property that belongs to the City.

Overall, areas to be strengthened include:

- ensuring security access request procedures are followed

- ensuring security incident reports are investigated and closed

- verifying that work orders are completed and closed

- monitoring contract compliance with security service providers

- ensuring payments to vendors are made in compliance with corporate procedures

- enhancing performance measures

- testing of site emergency plans

Conclusion

This report contains 21 recommendations to improve security and safety at City facilities. Areas to be strengthened are: physical security, access card processes, mobile patrol operations and security administration processes.

Finally, we would like to express our thanks for the cooperation we received from staff of the Corporate Security Unit during this audit.

BACKGROUND

Facilities Management Division is responsible for ensuring proper operation of all aspects of the City's facilities and to provide a comfortable and safe environment for the occupants. The division is comprised of four units reporting directly to the Chief Corporate Officer. Corporate Security's mandate is to provide security and safety services at City facilities.

Corporate Security provides security services at over 1,300 locations

Corporate Security services more than 1,300 City facilities. This includes City Hall, Metro Hall, civic centres, Union Station and divisional facilities. Front line security guard services are provided by trained corporate staff and by contract guards that include:

- providing onsite security at some facilities
- conducting investigations and preparing occurrence reports
- responding to alarms
- mobile patrols
- providing assistance to visitors

Corporate Security provides security devices at City facilities, including access control and alarm equipment, video surveillance equipment, and protection barriers. The maintenance of the access control equipment and video surveillance is covered under two separate vendor contracts.

Security Control Centre is the operations hub	Corporate Security also operates the Security Control Centre which is staffed 24 hours a day, seven days a week. Control Centre staff are responsible for:

- monitoring access to buildings and facilities
- investigating intrusion alarms
- monitoring video surveillance images
- dispatching security guards and/or contacting the appropriate first responders to emergencies

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

Audit objective	The Auditor General's 2014 Audit Work Plan included a review of Facilities Management – Security and Safety. The objective of this audit was to assess the adequacy and effectiveness of the physical security and safety measures at City facilities.
Audit Scope	We conducted our audit during the period of September to November 2014.

The audit focused on the following areas:

- Corporate Security operations
- physical security and safety measures
- access card controls
- maintenance of security systems and equipment
- training

Based on our risk analysis of the volume and severity of reported security incidents we selected facilities at two City divisions, (Toronto Water and Parks, Forestry and Recreation); to further review the physical security measures in place.

Audit Methodology	Our audit methodology included the following:

- review of security policies and procedures
- interviews with Corporate Security staff
- ride alongs with Corporate Security mobile patrols
- physical inspection of ten different City facilities
- evaluation of management controls and practices
- examination of documents and records
- review of security and emergency plans for two major civic centres
- review of contracts for the maintenance of security equipment
- review of audit reports issued by other jurisdictions
- other relevant audit procedures

Compliance with generally accepted government auditing standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDIT RESULTS

A. PHYSICAL SECURITY AT CITY FACILITIES

A.1. Physical Security Measures at City Facilities

This matter is being reported to Audit Committee in Confidential Attachment 1.

Recommendations:

1. **City Council request the Chief Corporate Officer to develop a plan to complete a review of physical security at all City facilities using a risk based approach and to address any deficiencies found during the review.**

2. **City Council request the Chief Corporate Officer to perform the appropriate follow up reviews to ensure identified security deficiencies are adequately addressed by the divisions.**

A.2. Site Information Packages Are Not Current

Site Information Packages used by control room operators

While on mobile patrol, security guards may visit a site they are unfamiliar with to investigate a security alarm/incident, reset security equipment or locate malfunctioning equipment. In such cases control room operators often refer to the site specific information packages located on-line to provide direction to mobile security guards.

Site Information Packages are not complete or accurate

In preparation for our site visits to review physical security at selected City facilities we obtained copies of the relevant site information packages. We found that even though changes had been made to facilities, 9 out of 10 site information packages did not have complete or accurate information including:

- incorrect description of site operational procedures
- incomplete or inaccurate listing of security equipment and its location
- outdated site contact information
- non-existent or outdated building floor plans
- one site information package was last updated in 2005

Recommendation:

3.   City Council request the Chief Corporate Officer to update Site Information Packages after significant changes have been made to a facility and periodically for all facilities.

A.3. Video Surveillance Equipment

This matter is being reported to Audit Committee in Confidential Attachment 1.

Recommendations:

4.   City Council request the Chief Corporate Officer to implement a process to ensure that all closed circuit television cameras not on the network are regularly checked and equipment deficiencies for all equipment are documented and repaired.

5.   City Council adopt the recommendation contained in Confidential Attachment 1 to this report.

B. ACCESS CARD CONTROLS SHOULD BE IMPROVED

B.1. Periodic Review of Access Cards

This matter is being reported to Audit Committee in Confidential Attachment 1.

Recommendations:

6. **City Council request the Chief Corporate Officer to regularly obtain employee termination reports from Corporate Human Resources and upon review cancel user access as required.**

7. **City Council request the Chief Corporate Officer to run reports to identify inactive access cards and upon review, cancel user access as required.**

8. **City Council request the Chief Corporate Officer to implement a review process for corporate sites to identify terminated access cardholders and remove access in accordance with security policies.**

B.2. Compliance with Card Access Request Procedures Should Be Improved

Some access approval documentation is incomplete

Granting physical access to City facilities is controlled through a multi-level approval process. All access card requests must be submitted to Corporate Security for processing. In a sample of request forms selected for review 2 out of 10 did not have the required information including proper approvals and access requirements. In addition the necessary supporting documentation for another access request could not be located.

Recommendation:

9. **City Council request the Chief Corporate Officer ensure that all access card request forms have the necessary information, access requirements and approvals completed before processing.**

C.   MOBILE UNIT OPERATIONS

C.1.   Mobile Patrol Staffing

This matter is being reported to Audit Committee in Confidential Attachment 1.

> **Recommendation:**
>
> 10.   **City Council request the Chief Corporate Officer to review the current level of mobile patrolling activity to determine if it adequately meets requirements and propose options for the actions, if any, necessary to satisfy the security needs.**

C.2.   Mobile Patrols

This matter is being reported to Audit Committee in Confidential Attachment 1.

> **Recommendation:**
>
> 11.   **City Council request the Chief Corporate Officer to update run sheets and develop a protocol to ensure that all City facilities are patrolled over a reasonable period of time by using a combination of scheduled and random patrols.**

D.   ADMINISTRATION PROCESSES COULD BE IMPROVED

D.1.   High Number of Open Security Incident Reports

Security incident reports should be closed once review or investigation completed

From January 2010 to September 2014 security guards generated 51,812 security incident reports on Corporate Security's tracking system. Supervisors are responsible for reviewing and investigating each incident report to the extent necessary. Upon completion of the review and/or investigation the supervisor should immediately close the incident report.

Incident reports not closed after completion

We noted that 7,144 (13.8%) incident reports were open of which 2,244 (31.4%) had been open for more than two years. Corporate Security advised that reports are only closed when no further action is to be taken. As an example, a report of a lost or stolen item would not be closed until the earlier of the item being located or approximately two years. This process makes it difficult to quickly assess open incident reports that require attention. We reviewed a sample of ten open incident reports and found that none required further action. Therefore, they should have been closed.

Supervisors indicated that they review security incidents the following day however due to workload may not have time to close them. Since the status of the incident reports in the system are not always updated the monthly statistical summary reports are inaccurate.

Recommendation:

12.   City Council request the Chief Corporate Officer to ensure that supervisors periodically run a status report for open incident reports and close them in a timely manner once resolved.

D.2.   Outstanding Work Orders, Work Orders Not Closed When Completed

Corporate Security has one maintenance contract for access control equipment and one for CCTV equipment. Each contract covers the cost of preventive and corrective maintenance service calls at predetermined sites.

Work orders not closed upon completion

Corporate Security's service desk tracks and monitors the status of each work order to ensure they have been completed in a satisfactory and timely manner. We analyzed all work orders created from January 2012 to September 2014 and found that 48 per cent of work orders had not been closed. The majority of work orders created in 2014 were closed. This improvement could be due to a newly created position at the service desk which includes a responsibility to monitor and track work orders.

*Outstanding
work orders not
resolved in over
a year*

Our review also determined that several work orders that were
the responsibility of one particular vendor, have not been
resolved. The contract requires that security matters be resolved
in 2 to 24 hours. Our analysis determined that out of 1678 work
orders issued over the past two years, 65 related to CCTV
equipment were still open. Delays in resolving work orders
could mean, for example, that CCTV cameras may not be
working at key City sites.

Management at one division indicated they were dissatisfied with
the amount of time required to fix CCTV cameras.
Malfunctioning equipment places City assets at risk.

> **Recommendation:**
>
> **13. City Council request the Chief Corporate Officer to
> periodically review work orders for the vendors
> responsible for the maintenance of security equipment
> that have been outstanding for longer than two weeks
> and to follow-up with the vendor to resolve
> outstanding deficiencies in a timely manner.**

D.3. Contract Management Practices Could Be Improved

*Maintenance
contracts need
improved
monitoring*

Corporate Security has contracts with two vendors for
maintenance of security equipment. According to the contracts,
valued annually at $2.1 million and $5.8 million, each vendor is
required to submit a monthly progress report to Corporate
Security. While meetings are held with the vendors to address
specific issues, the higher level monthly progress reports have
not been submitted since contract inception, (December 1, 2011
and July 1, 2014). The monthly report should include
comprehensive records on completed maintenance service, an
itemized list of service calls, charts and graphs indicating trends.
This information would be useful in monitoring vendor
performance and should be a factor considered in the selection of
particular vendors in the future.

> **Recommendation:**
>
> **14. City Council request the Chief Corporate Officer to
> request monthly reports and supporting
> documentation from the vendor and to review and
> monitor performance. When deficiencies are
> identified, appropriate corrective action should be
> taken.**

D.4. Overpayments for Time and Material Service Calls

Time and material service calls are not covered under the contract for maintenance of security equipment. These service calls are paid on a per usage basis, and the calls should be billed in accordance with the all inclusive labour rates quoted in the contract. No additional costs should be invoiced.

One vendor overcharged for service calls and paid

One vendor was charging a higher rate for time and material service calls than stipulated in the contract. The vendor charged a minimum of three hours labour for each service call and included additional charges for fuel surcharge and truck charge on each invoice. The hourly labour rate billed was $15 per hour higher than specified in the contract and the additional surcharges billed for each service call was $87.

Management did not detect overpayment errors

Overpayments were made to the vendor since the inception of the contract, July 1, 2014. As a result of our audit work Corporate Security is following up on the overbillings and we estimate that it will not exceed $10,000.

> **Recommendation:**
>
> **15.   City Council request the Chief Corporate Officer to review all time and material invoices billed since July 1, 2014 by the vendor and initiate recovery of any overpayments.**

D.5. Advance Payments Made to Vendor on Maintenance Contracts

Vendor paid for work not yet fully completed

A service contract for access control equipment and another for CCTV cameras and equipment were awarded to two separate vendors. We found that both vendors have invoiced, and Corporate Security paid, in advance for flat rate corrective and preventive work that had not yet been fully completed. According to Corporate Accounts Payable *"It is the City's payable practice to not pre-pay or make advance payments"*.

> **Recommendation:**
>
> **16.   City Council request the Chief Corporate Officer to ensure that payments for services are not made to vendors until all work has been completed according to the contract specifications.**

D.6.   Performance Measures Should Be Enhanced

Limited performance measures in place

Since 2012 Corporate Security reported out against two performance measures: the percentage change in number of security incidents year to year and percentage of security projects on time/budget.

Further meaningful performance measures should be developed

Additional key performance indicators may be helpful in measuring the effectiveness of security. Some examples might include:

- number of security assessments planned versus completed
- incident response time
- amount of time to close a file based on the type of incident

Corporate Security should review the key performance indicators used by other organizations, and implement the performance measures that will promote performance improvement, effectiveness, efficiency, and appropriate levels of internal controls and best practices.

The Unit's results over time should be compared against established targets, other municipalities and organizations and security industry benchmarks. This will assist management in evaluating the effectiveness of current operational practices and identify areas for improvement. Such information may be useful for setting strategic targets in the business plan.

Recommendation:

17.   City Council request the Chief Corporate Officer to further develop and implement performance measures that will promote performance improvement, effectiveness, efficiency, and appropriate levels of internal controls.

D.7.   Use of Force Training Refresh Not in Accordance with Unit's Objectives

To obtain an Ontario license to act as a security guard one must successfully complete a training program from an accredited provider. Such training is normally provided by a public university, college, private career college or licensed/registered business entity.

Use of Force techniques taught by Corporate Security

Security guards may be required to use force during certain situations. Corporate Security teaches hands-on use of force techniques as part of the two week mandatory orientation training program for corporate security guards. This training is consistent with the Ministry of Community Safety and Correctional Services training curriculum for security guards states that *"Students need to attend specialized training to learn how to use defensive equipment and to apply use of force techniques"*.

Use of force training requirements should be assessed

Annually, Corporate Security teaches a Use of Force refresher training course to corporate security guards. The course provides security guards an opportunity to practice such skills in a controlled setting. As of October 2014, 115 out of 136 security guards had not completed the refresher Use of Force training course in over one year. Management indicated that it was difficult to schedule security guards for the refresher course due to short staffing and a number of events requiring additional security. In addition, management advised that the goal for annual training is self imposed and will be reviewed as it may be too stringent.

Recommendation:

18.   City Council request the Chief Corporate Officer to review the current requirement for use of force training and make any necessary adjustments to corporate requirements.

D.8.   Incomplete and Decentralized Training Records

Corporate security guards are required to have specific job qualifications and training in order to qualify to work in security, including: a valid security guard license, valid first aid certificate, safety training and use of force training. These requirements are determined by provincial statute, regulations or Corporate Security job specifications.

Training records are not centralized

We determined that security staff training records are not centrally stored. Some training courses are not scheduled or recorded in the staff scheduling system. Training records are both accumulated in the scheduling system and on various spreadsheets that are maintained by different staff. In addition, first aid training records are maintained by Emergency Medical Services Cardiac Safe City Program.

We could not locate all of the safety training records and found tracking errors on certain training spreadsheets. Not having centralized training records makes it difficult to track and monitor whether employees have met training requirements and is prone to error.

> **Recommendation:**
>
> 19. **City Council request the Chief Corporate Officer to store all corporate training records for security guards in a centrally maintained database, to update training records in a timely manner and to monitor compliance with training requirements.**

D.9. Testing of Emergency Plans

This matter is being reported to Audit Committee in Confidential Attachment 1.

> **Recommendation:**
>
> 20. **City Council request the Chief Corporate Officer to ensure that emergency plans are tested by conducting drills or exercises for important portions of the plan and that the results be reviewed and changes be made to the plan accordingly.**

D.10. Some Corporate Security Policies and Procedures Are Not Current

Safety and security procedures provide guidance on roles and responsibilities, and they help to support effective decision-making, and ensure consistency in operations.

Some policies and procedures are not up to date

Our review showed that various Corporate Security policies and procedures did not reflect the current operational practices in place or were no longer valid, including the:

- Corporate Site Checklist Policy

- Audit and Inspections – Video Surveillance Camera Inspection Policy

- Policy and Procedure Manual for Corporate Security Scheduling

- The On-demand Maintenance Service Call Process, and

- Key Audits procedure

Recommendation:

21.   City Council request the Chief Corporate Officer to periodically update policies and procedures to reflect current operational practices, improvements to safety and security, and after any significant changes in processes or security incidents.

CONCLUSION

This report contains 21 recommendations to improve safety and security at City facilities. Areas to be strengthened include: physical security, access card processes, mobile patrol operations and the security administration processes.

Management's Response to the Auditor General's Review of
Facilities Management – Security and Safety Improvements Required

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
1.	**City Council request the Chief Corporate Officer to develop a plan to complete a review of physical security at all City facilities using a risk based approach and to address any deficiencies found during the review.**	X			This matter is addressed in a number of areas: a) Security Building Condition Assessments are done annually. Commencing January 2015, Corporate Security will expand their Security Building Condition Assessments to also capture immediate security compliance issues including propped open doors, poor lighting, etc and work with the applicable divisions to address the deficiencies. b) Testing is done on security system components based on the type of site and components (daily, weekly, monthly, semi-annually). Commencing February 2015, on site examinations will be expanded to include compliance issues. c) An annual schedule will be prepared by March 31, 2015 of various sites, chosen by level of risk, for in-depth review/audit in 2015.
2.	**City Council request the Chief Corporate Officer to perform the appropriate follow up reviews to ensure identified security deficiencies are adequately addressed by the divisions.**				Corporate Security will follow-up on outstanding security deficiencies in divisions by submitting a quarterly report to each applicable Division Head detailing metrics such as outstanding and completed deficiencies.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
3.	**City Council request the Chief Corporate Officer to update Site Information Packages after significant changes have been made to a facility and periodically for all facilities.**	X			Corporate Security has been implementing SharePoint since February 2014 to better manage documents and revision control. Site packages began moving to the SharePoint site since December 2014 to help organize and track site package information. The lifecycle of a site package will also be maintained. Each site package will have a life cycle pre-determined based on site specific criteria and client needs. Once the site package reaches its lifecycle the owner will be prompted by email to review and republish the document, if needed. This prompt will ensure the content of site packages are reviewed when required and information is kept up to date. At a minimum, all site packages will have annual reviews by the applicable Security Supervisor and metrics will be maintained.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
4.	**City Council request the Chief Corporate Officer to implement a process to ensure that all closed circuit television cameras not on the network are regularly checked and equipment deficiencies are documented and repaired.**	X			At the vast majority of City sites, video surveillance equipment is checked by Corporate Security on a daily or twice weekly basis. At a small percentage of sites, video surveillance equipment is not connected to the City network as no site network connection exists. For these sites, an applicable divisional staff member will be delegated for each site, by March 1, 2015, to perform a daily review of that site's system monitor as is the existing case with most non-networked sites. As a further enhanced measure, the Corporate Security Mobile Patrol will also be responsible to complete a documented physical check of the recording system twice monthly.
5.	**This recommendation is being reported in Confidential Attachment 1.**				

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
6.	**City Council request the Chief Corporate Officer to regularly obtain employee termination reports from Corporate Human Resources and upon review cancel user access as required.**	X			Completed. Beginning October 2014, Corporate Security implemented a new, daily process to ensure inactive employees on SAP had their security access disabled. A daily report is provided by Human Resources from SAP of inactive employees. Corporate Security staff then verify that the card access was deactivated on the system. As part of the 2015 IT workplan is the review of an automated process whereby the SAP information would automatically update the security system information.
7.	**City Council request the Chief Corporate Officer to run reports to identify inactive access cards and upon review, cancel user access as required.**	X			In 2015, a quarterly report will be run comparing the full active SAP database against the full security system database to review any possible errors. As part of the 2015 Operating Budget submission, is a request for a Security Guard to provide further staffing to Access Control Area.
8.	**City Council request the Chief Corporate Officer to implement a review process for corporate sites to identify terminated access card holders and remove access in accordance with security policies.**	X			A capital project will commence in 2015 to automate the current manual process for routine roster reports. This IT service management application will enhance the availability of roster reports for Designated Access Approvers.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
9.	**City Council request the Chief Corporate Officer ensure that all access card request forms have the necessary information, access requirements and approvals completed before processing.**	X			A communication will be sent out from Corporate Security to all Designated Access Approvers by February 20, 2015, re-iterating the applicable procedures as they relate to access and authorizations. A capital project will commence in 2015 to automate the current manual process for access authorization. This IT service management application will obtain and track access card request information, automate the access approver process of the Designated Access Approver, assist with managing the proper authorization databases, and provide City staff with easy to use on-line forms. An internal annual compliance audit will be performed using a sample listing of access approvals done in the current year.
10.	**City Council request the Chief Corporate Officer review the current level of mobile patrolling activity to determine if it adequately meets requirements and propose options for the actions, if any, necessary to satisfy the security needs.**	X			A review of mobile services will be conducted by April 30, 2015. This review will encompass delivery models, partnerships, and best practices.
11.	**City Council request the Chief Corporate Officer to update run sheets and develop a protocol to ensure that all City facilities are patrolled over a reasonable period of time by using a combination of scheduled and random patrols.**	X			The current protocol and practices will be reviewed as part of the Mobile Services review.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
12.	**City Council request the Chief Corporate Officer to ensure that supervisors periodically run a status report for open incident reports and close them in a timely manner once resolved.**	X			A monthly report will be run by Security Supervisors and reviewed by the applicable Manager. These metrics form part of the Security Supervisors' 2015 Performance Planners.
13.	**City Council request the Chief Corporate Officer to periodically review work orders for the vendors responsible for the maintenance of security equipment that have been outstanding for longer than two weeks and to follow-up with the vendor to resolve outstanding deficiencies in a timely manner.**	X			This protocol is currently being followed. All previous open work orders where the work was completed have been closed. To enhance management reporting, as part of the 2015 IT Workplan the current work order process will be migrated to an IT Service Management Application. This application will assist in the management of these work orders. This application will also allow for the provision of performance measures to be reviewed as part of the documented monthly meetings with the vendors.
14.	**City Council request the Chief Corporate Officer to request monthly reports and supporting documentation from the vendor and to review and monitor performance. When deficiencies are identified, appropriate corrective action should be taken.**	X			While documented monthly meetings occur with these vendors, Corporate Security will ensure monthly reports are provided. These reports will now be verified by the Business Analyst and will be annually audited for compliance. Letters will be sent to the applicable contractors reminding them of these requirements by February 20, 2015.
15.	**City Council request the Chief Corporate Officer to review all time and material invoices billed since July 1, 2014 by the vendor and initiate recovery of any overpayments.**	X			Completed.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: (Comments are required only for recommendations where there is disagreement.)	Action Plan/Time Frame
16.	**City Council request the Chief Corporate Officer to ensure that payments for services are not made to vendors until all work has been completed according to the contract specifications.**	X			A process change has occurred whereby all payments for services are now verified by two levels of approvals to ensure payments are only completed once all work is completed.
17.	**City Council request the Chief Corporate Officer to further develop and implement performance measures that will promote performance improvement, effectiveness, efficiency, and appropriate levels of internal controls.**	X			As part of the IT Workplan for 2014 and beyond are a number of programs either currently used by Corporate Security that have reached their end of life cycle or new programs required. These programs will automate the provision of metrics and performance measures. A review of metrics and performance measures commenced in 2014 and will be completed by March 31, 2015.
18.	**City Council request the Chief Corporate Officer to review the current requirement for use of force training and make any necessary adjustments to corporate requirements.**	X			A review of use of force training commenced in 2014 and will be completed by February 28, 2015. This review encompasses various different use of force delivery methods that permit smaller class sizes for easier scheduling, reviews the sharing of resources with other Agencies, Boards and Commissions, and reviews benchmarking and best practices.
19.	**City Council request the Chief Corporate Officer to store all corporate training records for security guards in a centrally maintained database, to update training records in a timely manner and to monitor compliance with training requirements.**	X			All Corporate Security training records will be transferred to the Staff Scheduling Program by March 31, 2015 and this program will become the central database. Metrics will be maintained from this database to monitor compliance with legislative and self-imposed training requirements.

Rec. No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
20.	**City Council request the Chief Corporate Officer to ensure that emergency plans are tested by conducting drills or exercises for important portions of the plan and that the results be reviewed and changes be made to the plan accordingly.**	X			For Corporate sites under the responsibility of the CCO, the COO will ensure Facilities Management conducts additional drills or exercises for applicable sites based upon a risk review. For non-Corporate sites, the CCO will notify the divisions of their obligations following the adopted recommendation.
21.	**City Council request the Chief Corporate Officer to periodically update policies and procedures to reflect current operational practices, improvements to safety and security, and after any significant changes in processes or security incidents.**	X			Corporate Security has been implementing SharePoint since February 2014 to better manage documents and revision control. Policy and procedural documents will be managed within the Corporate Security SharePoint site.