City of Toronto City-Wide Corporate Security Policy

2009

INDEX

7.0 CITY POLICIES OR PROCEDURES INVOLVING CORPORATE SECURITY

- 7.1 Security Video Surveillance Policy
- 7.2 Bomb Threat Procedures
- 7.3 Lockdown Procedures
- 7.4 Workplace Violence Policy

8.0 CITY POLICIES WITH SECURITY CONSIDERATIONS

- 8.1 Maintenance Standards
- 8.2 Fleet Safety Policy
- 8.3 Fraud Prevention Policy
- 8.4 Accessibility Design Guidelines
- 8.5 Graffiti By-Law
- 8.6 Corporate Access and Privacy Policies
- 8.7 Municipal Code, Chapter 629 Property Standards

9.0 APPLICABLE LEGISLATION AFFECTING SECURITY

- 9.1 Private Security Guard and Investigators Act
  - 9.1.1 Implications for the City of Toronto
- 9.2 Criminal Code of Canada
- 9.3 Trespass to Property Act

10.0 STAKEHOLDERS / PARTNERS

- 10.1 Corporate Access and Privacy Office
- 10.2 Community Safety Secretariat
- 10.3 Human Resources Division
- 10.4 Information & Technology
- 10.5 Insurance and Risk Management Unit
- 10.6 Purchasing and Materials Management Division
- 10.7 Law Enforcement Agencies

11.0 ADDITIONAL STATEMENTS

- 11.1 Complaints Process
  - 11.1.1 Complaints About Security Guards
  - 11.1.2 Complaints About Security Policy or Procedures
- 11.2 Access and Equity Hiring and Training
- 11.3 Civilian Oversight
- 11.4 Environmental Design

12.0 REFERENCES

1.0 INTRODUCTION

1.1 Policy Statement

The City of Toronto depends on its personnel and assets to deliver its vital services to the public and has an obligation to protect employees and the visiting public, preserve the availability of assets and assure the continued delivery of services in an effective, safe and sustainable manner.

As employees of the City, it's a shared responsibility to provide and maintain a safe and healthy work environment. Proper security is much more than protecting physical property, rather its greatest importance is in protecting the health and safety of employees, clients and the public who utilize City services. A safe City property also encourages public usage and civic engagement.

Organizational reputation, the uninterrupted reliability of the technical infrastructure and normal business processes, the protection of physical and financial assets, the safety of employees and customers, the degree of usage of City programs, the attendance at events, and the preservation of public confidence all rely in some measure upon the effectiveness of the security program.

The protective role of Security constitutes a service to the City. The value of such service is better measured by what incidents do not happen than by what does. As a service, security shall be designed to work with and enhance operations where possible. At City properties, it is imperative that security be appropriately balanced with accessibility, the implementation of security counter-measures be based on risk, and that the consideration and implementation of physical security measures be coordinated with an examination of root causes.

The City-Wide Corporate Security Policy prescribes the application of proactive and reactive safeguards measures, clear policies and procedures, stakeholder involvement, policy enforcement, the confidential nature of private security concerns or observations, and clear communication of Corporate Security expectations in order to met the above stated objectives.

1.2 Application

The City-Wide Corporate Security Policy applies to all City staff of City divisions. Certain sections of this Policy also apply to contracted Security Guards, contractors, and service providers where referenced.

1.3 Objectives

The purpose of the City-Wide Corporate Security Policy is to:

- provide and highlight the Corporate Security framework;
- outline the roles and responsibilities of City employees in keeping City assets secure;
- emphasize security policies and the responsibilities of various staff;
- highlight additional policies that relate to security;
- highlight relevant legislation and its effect on security at City facilities; and,
- provide statements on civilian oversight, independent complaints process, access and equity hiring and training, and environmental design measure.

This Policy does not provide complete, detailed Corporate Security and/or Security Industry standards and guidelines as they relate to security facility classifications, equipment specifications standards, installation standards, testing standards, monitoring standards, etc. These documents may vary depending upon the classification of facility and legislative requirements. Some of these documents are however referenced in "**Section 12: References"** of this document.

The Corporate Security Policy specifies two categories of requirements: mandatory and recommended. As a part of these requirements the word *shall* and *must* are designated as mandatory requirements and the word *should* as a recommendation (except where direct language is quoted from City policies, Acts, Codes, etc.).

As of December 2008, all editions of Policies, Acts, and Codes referenced in this document were valid. It is however recommended that the latest version of any references be verified prior to being quoted.

1.4 Scope

An integral part of security is the application of integrated protection afforded by the systematic identification and mitigation of risk. Through managerial, physical and operational practices, Corporate Security is able to deter, detect, and diminish risk to the safety of employees, clients, and the visiting public, as well as, the security of assets and information.

Security activities include, but are not limited to:

- identification of assets and critical infrastructure;
- threat, risk, and vulnerability identification and analysis;
- reporting, investigating, and recording of incidents;
- the creation of security plans, policies, and procedures;
- personnel and physical Security;
- protection of sensitive information and systems; and,
- liaison with intelligence and law enforcement agencies.

1.5 Definitions

Assets:
Employees, visitors, customers, facilities, structures, lands, City-owned property, devices, etc. Assets can be tangible and intangible.

Corporate Security:
A Unit of the Facilities and Real Estate Division.

Designated Access Approver (DDA):
A management employee designated by the Division Head to be responsible for authorizing access requests for a division, facility, or floor.

Security Guard:
A Security Guard under the Private Security and Investigative Services Act, 2005 is defined as "(4) A security guard is a person who performs work, for remuneration, that consists primarily of guarding or patrolling for the purpose of protecting persons or property. 2005, c. 34, s. 2 (4)."

2.0 BACKGROUND

2.1 City Council Decisions

April 20 & 23, 2007 Special Meeting of Toronto City Council

The Toronto City Council Decision Document for the Special Council Meeting of April 20 and 23, 2007 references a "City-wide security review" in 3 clauses:

- Under "Citizen Centred Services "A", Parks, Forestry and Recreation", Clause #12, "funding for future phases of the Divisional Safety and Security Plan be considered in the context of the **City-wide security review**;"
- Under "Toronto Transit Commission – Conventional", Clause #93, "the City Manager, in consultation with the TTC, Toronto Police Service and the Deputy City Managers, report back to Executive Committee, prior to the 2008 Operating Budget process, on a **City-wide security policy**, which addresses, among other issues, the use of TTC Special constables, such report to include input from the Chief of Police and Local Commanders from the at-risk communities; and"
- Under "Toronto Transit Commission – Conventional", Clause #94, "the Interim Chief General Manager of the Toronto Transit Commission report back to the Budget Committee, prior to the 2008 Operating Budget process, with a revised multi-year security strategy that would be consistent with a **City-wide security plan**."

March 31, 2008 Special Meeting of Toronto City Council

The Toronto City Council Decision Document for the Special Council Meeting of March 31, 2008 amends recommendations contained in a February 4, 2008 report from the City Manager, entitled "City-Wide Security Plan" and approved:

1. That further improvements and enhancements be made to the current Corporate Security framework with the objective of enhancing corporate standards and further centralizing those security functions which have City-wide implications.
2. The Corporate Security Unit undertake further consultations with the affected divisions and review existing divisional security plans and create plans for divisions currently without plans and report back in the fall of 2008.
3. Staff report to the Budget Committee in July 2008 on the comparator information and options utilized by other major cities, and that staff report on the framework and implementation as they relate to ABCs.

4. That the framework for the City-wide Security Plan include advice on civilian oversight, independent complaints process, access and equity hiring and training, and environmental design measure.
5. That the City Manager request all City Divisions to declare a moratorium on new Security Staff hirings for 2009 until the City's Security Plan is submitted to the Executive Committee.

2.2 Legislative Reasons for Security

Employees, customers, and the public expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functional lines to mitigate or reduce those risks.

The City of Toronto has a responsibility to provide and maintain safe and healthy working conditions by complying with all applicable policies, Acts, and Codes and that this compliance is documented and monitored to ensure applicable measures and actions are taken. The City of Toronto also has a duty to protect City of Toronto employees and members of the public from foreseeable dangers. Knowing the current and foreseeable threats may provide the City of Toronto with a duty to act and implement applicable counter-measures.

Some of the Acts/Codes where this duty is obvious, and can carry severe penalties when breached, include the:
a) Occupational Health & Safety Act
b) Criminal Code of Canada, Bill C-45
c) Occupiers Liability Act

The City of Toronto also has specific policies outlining these duties, including the:
a) Corporate Occupational Health & Safety Policy
b) Workplace Violence Policy
c) Working Alone Policy

<u>Litigation</u>
Aside from the aforementioned Acts, Codes, or Policies, the City of Toronto needs to be concerned with litigation. Employers are expected to maintain a safe work environment and civil action could result in the event of the City failure to maintain a safe workplace.

2.3 Security in Plans and Mission Statements

2.3.1 Council's Strategic Plan

The actions of City Council are guided by a number of principles. Two of these principles, *Community Participation* and *Effectiveness*, are impacted to some degree by security measures. In order to have active community involvement in civic life (Community Participation), individuals must feel safe attending City facilities, meetings, events, public forums, etc. As a part of the principle of Effectiveness, "…Council will safeguard public assets". Proper security is an important measure in helping to safeguard public assets.

Council's Strategic Plan also contains *Goals for the community*. One of these goals where the notion of security is an obvious contributor is *Safe City* where it details that: "Toronto must be a place where individuals and communities feel safe and secure". The City can lead by example in ensuring safe and secure City facilities.

2.3.2 Toronto Public Service Framework: Mission and Values

The mission of the Toronto Public Service is to serve a great city and its people. The Values of the Toronto Public Service are Service, Stewardship, and Commitment. One of the ways Stewardship is defined is "*by taking care of our resources* and *managing public money and assets responsibly"*. Security plays a key role is taking care of resources through their protection.

One of the five goals of the Toronto Public Service People Plan is "We will have safe and healthy workplaces". Proper security is key to having safe workplaces.

2.3.3 Facilities & Real Estate Mission Statement

"Our mission is to plan for, build, maintain and improve City properties in a manner that supports direct service delivery, safety and comfort to the users, and municipal pride in appearance."

Proper security is an important measure in assisting Facilities & Real Estate in fulfilling this mission.

3.0 CORPORATE SECURITY

3.1 Corporate Security Unit

The Corporate Security unit, under the Facilities and Real Estate division, is the corporate body responsible for setting security standards and partnering with City divisions for the protection of City employees and assets. This is completed utilizing a mix of proactive and reactive security measures (services). The sharing of resources, knowledge, and expertise allows for security to be provided in a standardized and cost-effective manner.

The Corporate Security Unit maintains a Security Control Centre that can be contacted 24 hours per day for the safety of staff and the protection of assets. The City-wide Security Emergency number is 416-392-6666 (2-6666), City-wide Non-Emergency number is 416-397-0000 (7-0000), and the Corporate Security Control Centre e-mail is "seccc@toronto.ca"

3.2 Mission Statement

"The Corporate Security Unit is committed to supporting and enhancing the safe delivery of City services. We do this by providing and maintaining an appropriate level of sustainable proactive and reactive security and life safety measures through highly qualified, knowledgeable, trained security professionals, contracted services and current technology."

3.3 Services

The majority of services provided by Corporate Security fall into seven major categories:

3.3.1 Audits and Assessments

- Provide detailed security risk assessments and building security condition assessments.
- Complete Crime Prevention Through Environmental Design (CPTED) assessments.
- Develop physical protection system capital plans, system design, implementation, and training following physical security standards.
- Provide guidance, assistance and direction to employees and sub contractors on facility construction and renovation projects.

3.3.2 Security Systems

- Specify physical security measures according to standards, guidelines, and best practices.
- Implement physical security measures (locks, keys, barriers, alarm systems, access control systems, video surveillance, communication, lamination, lighting, etc.).
- Maintain and program City of Toronto access cards and card readers.
- Oversee security device preventative maintenance and repair.

3.3.3 Staffing

Corporate Security provides a wide range of security staffing options through in-house and contracted services for City-owned and leased properties. These options include:

- Security Mobile Alarm Response.
- Security Mobile Patrol.
- Contract Security Guard management.
- In-house Corporate Security Officers (Security Guards).
- In-house Control Room Officers.
- Security program supervision.

3.3.4 Security Control Centre Operations

The Corporate Security Control Centre is the hub of all Security operations for the City of Toronto. Staffed 24 hours a day, seven days a week, the Security Control Center provides a wide range of services, including:

- Monitoring access to City properties through various security systems and measures.
- Responding to and investigating alarms or abnormal usage.
- Monitoring video surveillance systems.
- Dispatching appropriate staff and mobile responses to emergencies and contacting the applicable emergency service.

3.3.5 Incident Response

To ensure security incidents are appropriately documented, investigated, tracked, and closed, Corporate Security completes:

- Incident reporting / recording.
- Investigations of security incidents or breaches.
- Recommendation ad implementation of security measures.
- Follow-up and closure of incidents.

3.3.6 Training

Corporate Security offers a number of security training programs including: Security Orientation, Crime Prevention, Theft and Robbery Prevention, Workplace Violence, Domestic Violence, Crisis Intervention, and Conflict Management.

3.3.7 Other

Other services provided by Corporate Security include:

- Security Event Planning.
- Event Security.
- Emergency Plans.

3.4 Corporate Security Framework

This framework involves mandating that the Corporate Security Unit, under the Facilities and Real Estate division, is the corporate body responsible for setting security standards and protecting assets for City divisions.

Under this framework, the centralization of the security function allows existing and future security resources to be properly coordinated, shared and responsive towards those areas in demonstrated need according to threats, thus augmenting the overall level of security.

Corporate Security will partner with City divisions to provide and enhance the safety and security of divisional employees, clients and assets. Divisional Security Plans are continually referenced and updated to guide specific divisional security needs.

This framework serves as the basis for the Corporate Security Policy as it relates to:

- the requirement for security plans;
- the methodology for the development of security plans;
- the requirements for specific security policies; and,
- the requirement for specific statements on civilian oversight, independent complaints process, access and equity hiring and training, and environmental design measures.

This framework provides a template for an Agency, Board, or Commission to create and adopt it’s own Security Policy in order to further enhance the protection of it’s assets through proactive and reactive security measures.

4.0 DIVISIONAL SECURITY PLANS

4.1 Purpose

The Divisional Security Plan is a joint document created and updated between Corporate Security and each division. Each division is responsible for the designation of key individuals to represent the division in this process

Each Divisional Security Plan is intended to be a fluid document that has its priorities reviewed and updated at least annually based on changes in threats, security occurrences, security measures implemented in the previous year, and new legislative or policy requirements.

Each Divisional Security Plan shall be referenced to guide future year divisional operating and capital requests based on operational priorities and within approved budget levels. Divisions shall be engaged throughout the implementation of their plan through Service Level Agreements, applicable meetings, and other required structures or processes.

4.2 Methodology

Corporate Security uses a methodology to update and create divisional plans involving:

a) Data Gathering

Required data gathering and analysis is completed by:

- Working with key contacts for divisions to obtain further background on their operating and physical security including statistics of incidents, obvious deficiencies, roadblocks to further enhancements, and special requirements of certain classifications of facilities or areas in their division.
- Obtaining relevant City-wide statistics through City insurance loss reports, H&S reports, Security incident reports, and Police incident statistics to be help determine the level of threats for different areas.

b) Identification / Prioritization of the Threats

- Identification / prioritization of the various threats / risks posed and the evaluation of the current measures in place to counteract these threats (a threat assessment). A security threat assessment of the facility shall follow a recognized documented risk assessment methodology such as the "General Security Risk Assessment Guideline" from ASIS International.

c) Security BCA's

- Completing the first stage of a Security Building Condition Assessment (Security BCA). A Security BCA is similar to a regular state of good repair building condition assessment; however, its sole focus is on security, an area not covered by on-going state of good repair BCA's. A key factor in the Security BCA is determining the security counter-measures that should be used. The "Corporate Security Assessment Methodology for Building Classification" provides this roadmap and can be used to help document the physical and operating security measures currently in place at the facility, provide the baseline standard for the facility type, and thereby highlight the areas below the standard.

d) Standards Development

Required standards development is completed by:

- Devising applicable security standards, practices, policies, counter-measures, and capital plans to enable the division to mitigate the risks which those threats present.

Based on the above data, a Divisional Security Plan is created for each division that:

1) Documents the current security features in place for each facility;
2) Completes a threat assessment by analyzing statistics, reports and operating risks;
3) Determines the security features required to address the risks highlighted in the Threat Assessment, with consideration given to industry standards and benchmarks;
4) Highlights the gap between the current security features and the recommended security features;
5) Presents a multi-year operating and capital plan to achieve the recommended security features in a suggested priority sequence; and,
6) Provides a multi-year operating and capital plan to maintain the recommended security features.

5.0 ROLES AND RESPONSIBILITIES

5.1 Chief Corporate Officer

The senior staff member responsible for the Corporate Security Policy is the Chief Corporate Officer. The Chief Corporate Officer is responsible for:

- on-going review and administrative updates of the Corporate Security Policy and security direction for divisions;
- ensuring compliance of this policy;
- allocating sufficient staff and other resources to appropriately secure City assets; and
- authorizing Corporate Security to move to an elevated Security level as required.

5.2 City Divisional Management Staff

Management staff of City Divisions shall**:**

- understand and uphold the principles of this Policy;
- ensure that all staff are familiar with their roles and responsibilities in the event of a security incident;
- ensure all employees are aware of how and when to contact Corporate Security;
- ensure all employees are aware of site security measures and their applicable usage;
- ensure all security related incidents are reported promptly to Corporate Security;
- ensure all potential threats to employee safety and security are reported promptly to Corporate Security;
- identify critical assets and threats within their divisions;
- with the assistance of Corporate Security, take all reasonable and practical measures to protect assets;
- identify and communicate security training needs to Corporate Security.
- provide for or release staff to take appropriate security-related training for the threats and risks encountered or likely to be encountered during their work activities; and,
- ensure City issued access cards and/or keys are taken from employees upon termination, leave or retirement;

5.3 Corporate Security

Corporate Security shall:

- provide a governance role to ensure adherence and compliance with the Corporate Security Policy, security regulations and applicable policies and procedures;
- manage the Corporate Security Program and act as a corporate focal point for all program security requirements;
- ensure the Corporate Security Program is continually updated to maintain relevance and currency;
- provide security to City-owned or operated properties through various security systems, a diverse contingent of in-house Security Officer and contracted Security Guards, and various contract firms / services;
- partner with divisions in developing and maintaining their sites' security;
- support City divisions in the furtherance of divisional goals by providing required security support to programs and projects;
- maintain an ongoing awareness of security standards, best practices, legislative and regulatory requirements, and developments in the security industry and update City standards accordingly;
- develop, and enhance corporate, divisional, and program specific standards, requirements, protocols, policies, and procedures to properly provide and enhance security for assets, employees and property;
- conduct security audits and assessments reviewing divisional, facility, or process security measures through assigned specialized personnel;
- manage capital security projects through assigned, specialized personnel and contractors;
- identify, test and implement tools, programs, and technologies to provide cost-effective solutions in order to meet identified critical and long term security needs;
- manage and co-ordinate security services to the Mayor, Council, visiting dignitaries, and City staff;
- conduct and manage applicable security investigations and act as a liaison with law enforcement personnel;
- collect and maintain records of losses, threats and security breaches and investigate and report on these as required; and,
- provide recommendations to the Chief Corporate Officer for update of the Corporate Security Policy.

5.4 Contracted Security Guards

Contracted Security Guards working on City-owned or operated properties shall:

- comply with all applicable regulations contained in the "*Private Security And Investigative Services Act, 2007*";
- comply with all expectations outlined in the service contract or bid award between the City and the contracted guard company and issued post orders, policies, and procedures;
- comply with applicable City policies which reference obligations of contractors (e.g. the City's Security Video Surveillance Policy);
- maintain the utmost professionalism, customer service, and confidentiality when dealing with employees and visitors; and,
- complete incident reports and distribute to pre-designated Corporate Security staff.

5.5 Contractors and Service Providers

Contractors and Service Providers working on City-owned or operated properties shall:

- comply with applicable City policies which reference obligations of contractors (e.g. the City's Security Video Surveillance Policy "A breach of this policy by service providers (contractors) to the City may result in termination of their contract"); and,
- comply with site specific security policies and procedures, including, but not limited to, access procedures, wearing issued identification, not taking facility keys or cards off the site, etc.

5.6 All Employees

All City employees are responsible for following the Corporate Security Policy and other security policies and procedures in the execution of their duties. All City staff shall:

- adhere to the Corporate Security Policy;
- maintain a safe work environment and work safely with consideration to security;
- remaining aware of their role as a safety and security partner by ensure all potential threats to employee safety and security are reported promptly to Corporate Security;
- ensure all security related incidents are reported promptly to Corporate Security; and,
- not tamper with or bypass any security measure.

6.0 SECURITY POLICIES & PROCEDURES

6.1 Application

The Corporate Security Unit shall be the primary contact and administrator of the policies and procedures contained in this section. These policies and procedures may be frequently updated based on upon operational need, new standards, or changes in City policy.

6.2 Security Threat & Risk Assessments

A wide array of issues should be analyzed before security measures are implemented, ensuring an appropriate distribution of resources, while not creating new exposures in the process. Through the Threat & Risk Assessment process, a range of threats, risks, and vulnerabilities are identified and categorized on the basis of criticality. These are organized so that Security measures are applied in a complementary and supportive manner to improve security based on risk priority.

Threat Assessment

Each Threat Assessment should follow a standard Threat and Risk Assessment template and procedure that encompasses at least the following four phases: asset definition; threat assessment; vulnerabilities analysis; and, selection of security measures. The overall objective is to define security requirements and to organize those requirements in a prioritized ranking.

Risk Assessment

A recognized risk assessment methodology shall be followed. See "**Section 12 References:** ASIS General Security Risk Assessment Guideline"

Recommendations

Recommendations for security measures shall be provided after an applicable threat and risk assessment. These security measures will vary depending on the building type, acceptable levels of risk, threat assessment results, cost-effectiveness, and standards.

Facility Design and/or Construction

Security must be fully integrated early in the process of planning, selecting, designing and modifying facilities. It is important to ensure that security is thoroughly addressed as part of an ongoing process for existing facilities, on any occasion where there is a change proposed to an existing facility's design and in all phases of an applicable construction or modification project. A Security Threat and Risk Assessments shall be conducted in the design phase for new facilities, as part of an ongoing process for existing facilities, and on any occasion where there is a change proposed to an existing facility's design or use.

Review of Assessments

Security Threat and Risk Assessments should be undertaken whenever a change is made to the design or structure of a facility, the use of the facility changes, the perceived threat level changes, or ideally at least once every 5 years.

6.3 Physical Security Design

The level of physical and operational security shall be established on a case by case basis based on a number of factors such as the results of a threat assessment, internal security best practices, external standards and benchmarking, City policy, stakeholder input, and cost-effectiveness.

A key security design principle is to provide a balance of accessibility and asset security. It must be understood that critical infrastructure, such as Water facilities, will have greater security and less accessibility than public City facilities where a greater mix of accessibility and security is required. The security requirements will vary depending upon facility type as each type faces varying threats and may require unique safeguards to provide adequate security against those identified threats.

6.3.1 Security Considerations

Most City of Toronto public facilities were built with open access and were never designed to be protected against the security threats and issues faced today. The complexity of today's security risks creates a diverse matrix of interrelated threats, vulnerabilities, and impacts. A number of considerations that should be taken into account when designing security measures is included below.

Root Causes

Examination should be completed into what possible root causes exist for current threats and security breaches. Consideration needs to be given to both internal and external threat factors and changes that have an overall effect on site security. Areas that should be examined include neighborhood facility changes, staff or resource reduction, changes to site operating hours, etc.

Impact on the Neighborhood

Once a range of security measures is proposed, consideration needs to be given to their possible effect on site security and the neighborhood. There are security measures that can either have positive or negative effects based on their design, type, and placement such as surveillance cameras, fencing, planters, barriers, parking control, window protection, procedures, and staffing. The ultimate goal of planned security measures is to increase overall site security while receiving staff and public buy-in, acceptance, and usage.

Address the Key Problem

Once a security measure is proposed, a review should be completed to ensure that the measure proposed will properly address the threat. This not only impacts the type of security measure but also the placement. This review must take into account privacy, accessibility, initial cost, required maintenance, longevity, aesthetics, interoperability, and integration.

Early Detection

An important principle of detection, delay and response, is to detect an intruder as early as possible, delay the intruder as long as possible through physical measures, and respond as quickly as possible. The ultimate goal should be to elongate the time between detection and the intruder reaching the asset so responders (Security, Police, etc) can intervene and apprehend.

Integration

Security measures shall be integrated where possible to enhance deterrence, detection, delay, and response.

Interoperability

An important consideration in the design and specification of equipment shall be whether the new equipment will easily integrate with existing site security equipment in order to allow interoperability to occur. Important considerations relate to make and model of equipment, availability of parts, ease of repair, and preventative maintenance.

Layered Protection

Consideration must be given to layering security measures to act as a back-up to, or a compliment to, existing equipment in order to enhance deterrence, detection, delay, and response.

Emerging Technology

A key consideration for security measures is ensuring the measure chosen is current and can be easily upgraded. It is important when choosing security technology that the company manufacturing the product be committed to the on-going and future support and development of the technology. As new technology is constantly emerging it is important that this technology is tested and evaluated in real operating conditions at City property before a commitment is made to wide usage.

Sustainability

It is imperative that prior to implementing security measures consideration be given to the sustainability of those measures. It must be recognized that some security measures have additional life cycle costs such as repair, maintenance, preventative maintenance, and replacement and the impact of these costs must be planned.

Crime Prevention Through Environmental Design (CPTED)

CPTED is defined as the proper design, effective use and maintenance of the built environment that can lead to a reduction in the incidence and fear of crime and an improvement in the quality of life and sustainability of land use. CPTED's goal is to solve crime-related problems before they exist, by planning & designing the physical environment to eliminate or reduce opportunities for crime. How the physical environment is planned and designed will have a strong influence in creating a safer place where people will involve themselves, participate in & take ownership of. CPTED is an important measure that should be considered prior to, and in concert with, other security upgrades.

Standards, Guidelines, Best Practices, and Benchmarking

There are a number of legislative, regulatory, and industry security standards, guidelines, and best practices affecting various area of security. These standards, guidelines, and best practices shall be considered during all phases of security including design, procurement, implementation, installation, programming, testing, and maintenance. See "**Section 12 – References**" for a list of Applicable Standards, Guidelines, and Best Practices.

Other Considerations

Upon the design of a system there are a number of smaller, yet important considerations that shall be taken into account. Consideration shall be given to:

- ensuring the measure proposed will be vandalism and damage resistant;
- the need for instructional signs, symbols, and language;
- lighting to ensure the measure will function appropriately in day and night conditions;
- device colour, as individuals may attribute certain colours to certain items (e.g. persons will be more hesitant to push a red exit button than a green one);
- the probability of a number of false or mischief alarms; and
- applicable usage (Will the security measures be appropriately used, tested, etc?)

6.3.2 Security Levels and Access Zones

Facility security should be designed in order to move between at least two levels of security: normal and elevated. Normal levels are moved to elevated by the securing of key areas, staffing, and procedures where the overall threat risk level for the facility is raised based on threat information, unexpected exposures, or actual incidents.

6.3.3 Access Control Zones

Facility security should be designed to encompass at least three access control zones to limit access to critical areas. These zones are completed through access control, barriers, and/or signage.

Public Zone	Free access to the general public.
Restricted Zone	Limited to employees and authorized persons.
Security Zone	Limited to specified employees or persons who have a need for access.

The mechanisms and procedures for restricting access to the various zones shall be commensurate with the level of risk associated for each zone.

6.3.4 Common Design Measures

Exterior and Interior Signs

Facilities shall display signs that give clear delineation between public and employee only space. Some types of signs are required by City Policy (Security Video Surveillance Policy), City By-Laws, and in order to effectively enforce Acts or Codes (such as the *Trespass to Property Act*).

Stairwells and Elevators

Stairwells and elevators should not provide direct, unrestricted access to restricted zones or Security zones. Where possible, passenger and freight elevators (including those from parking and loading dock areas) should open into a public zone.

Where applicable, access to work spaces from elevator lobbies shall be controlled in respect of employees, contractors, visitors and service personnel. Safeguards vary, depending on the nature of program, assets, the size of the work space, and the number of people requiring access to a floor. Additional security measures may include a physical barrier (such as a wall), an arrangement using personnel, or a reception function.

Pedestrian Entrances and Entrance Lobbies

Public entrances to facilities should be reduced as much as possible in order to channel traffic through a selected entry and exit point in order to effectively screen visitors and provide better service.

Service and Utility Entry and Exit Points

Service and utility entrance and exit points (such as air intakes, mechanical ducts, roof hatches and water supplies) should be safeguarded to ensure that the facility's critical assets and life safety measures are not compromised by unauthorized or uncontrolled access.

Shipping and Receiving Areas, Loading Docks and Mail Rooms

Where possible, shipping and receiving areas, loading docks and mail rooms should not be directly linked or adjacent to restricted-access areas or critical facility infrastructure.

6.4 Security Building Condition Assessments (Security BCA's)

Since typical Building Condition Assessments only review the status of existing systems and not the need for new security components where none existed previously, a different assessment methodology is required for security - Security Building Condition Assessments (Security BCA's). Security BCA's begin with a Security Threat Assessment of the facility following a recognized documented risk assessment methodology.

Security Building Condition Assessments shall be completed by specialized Corporate Security staff as part of the divisions' scheduled Building Condition Assessments.

6.5 Security System Procurement and Replacement

Where divisions recommend or require that a security or alarm system for a facility or area be procured, installed, moved, altered or replaced, Corporate Security shall be the primary contact. Before any system is designed or procured, a Threat Assessment should be completed to ensure the appropriate security counter-measure is in fact being recommended. Corporate Security will also ensure that applicable security standards, guidelines, and best practices are followed in regards to the threat assessment and system specification, design, integration, installation, and programming.

Where access control or alarm systems are required, the Corporate Security standard system will be used across all divisions and facilities, and employees will have one card for access to City facilities based on delegated authorities residing in each division's business units.

6.6 Security Staffing

Under the new Private Security and Investigative Services Act, 2007, persons or staff that provide security must be licensed as a security guard. This includes City staff and contracted services.

Where security staffing requirements exist for City divisions, the provision of these services must be provided through Corporate Security via the use of internal security resources or a contracted service, the determination of such to be based upon factors such as the result of a

security assessment, common past practice, history of risk exposure, and unforeseen emergent events (e.g. elevated level of security).

Corporate Security, with the assistance of the applicable division, shall prepare Standing Post Orders that fully describe the duties and reporting requirements for each security staffing position allocation.

Where the immediacy of an incident or event requires the dispatch of security staff, City divisions shall contact the Corporate Security Control Centre (416-397-0000) and provide the full duty requirements.

6.7 Alarm Monitoring

This Security Control Centre shall be responsible for monitoring the various City facilities' security alarm systems, card access systems, and security video surveillance systems. All security alarm systems at City facilities with the capability to be monitored from the Security Control Centre shall be monitored by Corporate Security. City division facilities with systems that are unable to be monitored by the Corporate Security Control Centre because of proprietary software, pre-existing contracts, or other reasons, shall have the management of these systems completed by Corporate Security.

New installations of security systems shall follow Corporate Security standards for assessment, design specification, installation, integration, monitoring, and maintenance.

6.8 Access Cards and Identification

Where access cards and/or identification cards are required, the Corporate Security standard shall be utilized.

There are two types of City of Toronto photo identification: 1) Access cards and 2) ID-Only cards. Access cards are used by staff that are authorized to have access at locations that are secured by access card readers, while ID-ONLY cards are used by staff that do not have to enter these locations but still require City identification. The major rules and regulations for both cards are the same and can be found on the reverse side of the card. Corporate Security

may also issue special customized identification cards to conform to legislative or program requirements. These custom cards must be coordinated with Corporate Security and are intended to remain separate from the standard issued access or ID-Only cards.

Each employee is responsible for their issued access card including appropriate use, maintenance, storage, and possession. Employees shall use their own access card each time they are entering a secure area. Employees shall not enter behind another employee or allow other persons to enter behind them (piggybacking). Since access levels can change frequently, an individual who may have had previous access to a floor or area may no longer have access or may no longer be employed by that division or even the City.

6.8.1 Obtaining an Access/Identification Card

City employees staying three months or longer are eligible for an employee access/identification (ID) card. To obtain an access / ID card, employees must attend a badging session with a completed "*Request for ID Card Form*".

6.8.2 Badging Regulations

No appointment is necessary, an employee shall however attend one of the badging sessions listed on the City's intranet site with their City of Toronto employee number and one piece of personal photo ID, including: drivers licence, passport, Citizenship card, Permanent Residence card, or photo health card.

Hats and sunglasses are not permitted in the photo. Badging sessions are not held on statutory holidays and may be cancelled without notice.

6.8.3 Reporting a Lost or Stolen ID Card

It is imperative that an employee immediately report to Corporate Security (416-397-0000) as soon as they realize their ID card is misplaced, lost or stolen. Once notified, Corporate Security will remotely disable the card, help the employee obtain a temporary replacement card, and request a new card be issued.

If an employee finds their previously misplaced card they should not attempt to use this card as it will be disabled and will cause a security alarm. The employee should instead notify Corporate Security so the card can be properly reactivated.

6.8.4 Reporting a Defective ID Card

If an access card becomes damaged or stops working, the employee shall attend the on-site Corporate Security desk at their work location. At facilities without on-site security staff, the employee shall e-mail "Security Access" (secacc@toronto.ca) to report the defective card and make arrangements for a replacement.

6.8.5 Requesting Additional Access

The level of access must be commensurate with job responsibilities and frequency of required access with the general principle being that only the minimum access on cards is provided for the employee to properly carry out their normal duties.

Employee cards are programmed to provide access to an area required for their job duties through authorization from their division's or unit's Designated Access Approver (DAA). Whereas additional access is required for work purposes, the employee shall make this request through that area's Designated Access Approver. That DAA will send an e-mail to "Security Access" (secacc@toronto.ca) listing:

- the name of the person requiring the access;
- exactly what access is needed;
- the hours access is to be granted; and,
- why the access is required.

If an employee is unaware of that areas Designated Access Approver (DAA) the employee should e-mail "Security Access" (secacc@toronto.ca) who will forward the e-mail to the DAA for authorization and contact the employee once the request has been fully processed.

6.8.6 Maintaining the Currency of the Card and Database

An access card will grant or deny access based on the information immediately obtained from the access card system database, thus making the currency of the database of utmost importance. It is important to note that just because an individual has an access card or ID-Only card in their possession does not mean that the individual is still actively employed by the City.

Each employee is responsible to ensure their information on the access card and the information provided to Corporate Security upon card enrollment is kept up to date. An employee shall notify "Security Access" (secacc@toronto.ca) to report changes to name, division, unit, work location, phone number, license plate number, and emergency contact information.

Each division is responsible for authorizing access, notifying Corporate Security of access additions or deletions, and notifying Corporate Security when an employee has changed sections, divisions, or is no longer employed by the City of Toronto.

Each management employee is responsible to immediately notify Corporate Security when an access card is to be temporarily suspended or terminated. Management staff shall obtain an employee's access card, keys, and any other City-owned equipment from an individual leaving the employ of the City. Divisional management staff shall immediately notify Corporate Security of the possession of the access card and keys and return these to Corporate Security. Divisional management staff shall immediately notify Corporate Security when an individual leaves the employment of the City and has not returned their issues access card, keys, or other applicable equipment.

6.8.7 Rules and Regulations

All employees shall adhere to the rules and regulations of access and ID card use that are printed on the back of access cards and ID-Only cards. These rules and regulations read:

1. This ID is the property of the City of Toronto and must be visibly worn while on City of Toronto property.
2. It must be presented upon request of Security or Management personnel.
3. If this ID is lost, stolen or damaged, notify Toronto Corporate Security immediately at 416-397-0000 (24hrs.)
4. This ID is for your personal use only, and is NOT TO BE LOANED TO ANYONE, NOT TO FAMILY, FRIENDS OR COWORKERS.
5. This ID must be returned to Corporate Security upon termination, leave or retirement.

Access and ID Cards must be worn with the front (photo) side of the card facing out. Cards are to be worn with the lanyards provided by Corporate Security or other lanyards with easy break-away features.

Employees are not authorized to loan out their cards or use cards of other employees. Each employee is directly responsible for their card at all times. Cards found in the possession of anyone other than the direct owner of the card will be confiscated by Corporate Security. Once the card is confiscated it will be investigated to determine if the card was lent or stolen. If the card was lent, Corporate Security will notify all Designated Access

Approvers (DAA) for all floors and divisions of access found on the card. Lending out or mismanagement of the card may lead to disciplinary action.

It is imperative that employee access and ID cards be returned upon termination, leave or retirement. Not only is this a matter of assisting with integrity of the card database but also cards can be recycled by being deleted and used again.

6.9 Alarm Response

Mobile security patrols and alarm response must only be completed by or contracted through Corporate Security. For legislative and health and safety reasons, non-Security employees shall never attend a site to respond to a security alarm. A licensed Security Guard is required to respond to alarms and all response shall be dispatched through Corporate Security. In case where internal facility access is required and Corporate Security does not have a key, a key holder (City employee) may be called to attend the site and meet Security to provide access, but only after the site has been investigated and deemed safe.

6.10 Incident Reporting

Corporate Security maintains an internal incident reporting system where all security incidents are to be reported. These occurrences reports are to be created for any security incident involving employees, visitors, or contractors while on City property or in the conduct of City work duties. These reports prove critical in documenting, investigating, and forecasting occurrences in order to assist the City in defending liability and displaying due diligence.

The collection and organization of information gathered from security incident reports is fundamental in determining where additional security resources are required in order to respond to applicable threats or actions. Sample incidents that are generated include, but are not limited to, crimes against people (public and employees), crimes against property; workplace violence, suspicious activity, medical emergencies, security policy breaches, and access control occurrences.

Reporting Mechanism

All security incidents shall be reported to Corporate Security in order to be documented and/or appropriately investigated. Incidents can be reported to on-site Security, or if none is available to the Corporate Security Control Centre by phone (416-397-0000) or e-mail seccc@toronto.ca .

Whereas a division or section already has in place a documented method of creating reports for security incidents due to operational or legislative reasons, Corporate Security will work with the division or section to capture the required information without unnecessarily duplicating workload.

Providing Reports

Some types of incident reports are provided to the Toronto Police Service or other law enforcement based on the need to report criminal activity. Incident reports pertaining to serious or suspicious incidents involving City of Toronto critical infrastructure may be shared with law enforcement agencies through the Royal Canadian Mounted Police, Suspicious Incident Reporting tool (S.I.R.).

Some incident reports, or the analysis of incident reports, may be shared with other City divisions or units based on operational need or in compliance with City policy. Such divisions or units include but are not limited to: Insurance and Risk Management, Human Resources, Occupational Health and Safety, Legal Services, and the Auditor General's Office.

6.11 Investigation and Reporting of Incidents and Threats

Corporate Security is responsible to investigate reported security incidents involving employees, visitors, or contractors while on City property or in the conduct of City work duties. City staff shall comply with the all aspects of the investigation. Depending upon the type and severity of the incident, the investigation may involve, or be passed onto, other divisions or units including: the Auditor General, Labour Relations, the Human Rights Office, senior management staff, or the Toronto Police Service.

It is imperative that employees report situations that that believe may lead to future security incidents or an unsafe workplace. Highly confidential situations can be directly reported to the Manager, Security & Life Safety, who can be reached through the Corporate Security Control Centre at 416-397-0000.

6.12 Key Control

It is imperative that appropriate door locks and keys systems be used at City facilities and that appropriate key control and key management policies be implemented. Whenever key control is lost for a lock, door, area, or facility, that lock or group of locks must be re-keyed. Examples of lost key control include: someone leaving the City and not returning their key, a lost key, unauthorized duplicates of a key made, or having keys that were unaccounted for.

High Security Locksets and Keys

When a building or lockset is required to be re-keyed, a high security lockset and key way is required. High security locksets are normally highly resistant to break-in, lock bypass, and lock picking. High security keys are normally highly controlled making them hard to duplicate.

City-Owned Keyway

Corporate Security utilizes a few restricted, high-security keyways owned by the City of Toronto. This helps ensure that key control is maintained and keys are not easily duplicated.

Key Duplication

Keys need to be appropriately stamped and tagged. All keys shall be coined or stamped with “Do Not Duplicate”. No person issued a City key shall attempt to duplicate the key by any means.

Employee Key Issuance

Whenever a key is issued to an employee for long-term use a *Key Issuance Form* (located on the Security & Life Safety intranet site) must be utilized in order to keep track of issued keys. This form contains conditions which the key holder must agree to. City staff responsible for issuing keys shall use this form, or a similar type that details the following conditions:

1. Issued keys remain the property of the City of Toronto.

2. The copying or lending of keys is strictly prohibited.
3. Lost or missing keys must be immediately reported to the Security Control Centre at 416-397-0000.
4. It remains the responsibility of the key holder to ensure reasonable and diligent care is exercised to ensure proper key security is maintained.
5. Corporate Security (or the person responsible for issuing the keys) may recall or replace issued keys without notice.
6. By signature for the keys, the key holder acknowledges that he/she has read and will abide by the above noted conditions.

Key Storage and Temporary Issuance

All keys, key blanks, key codes and keying charts not in immediate use must be securely stored.

Whenever a key is issued temporarily (less than 24 hours) that key shall be appropriately signed for and logged in an applicable Key Log. The number of keys on the ring need to be counted before issuance and re-counted when returned to ensure all keys are present. Persons being issued keys (employees, contractors, etc) must acknowledge that they will not take any keys off the key ring, will not use the keys to enter any area that are not authorized to enter, and will not take the keys off the site.

As in the case for access levels on access cards, only the lowest possible level of key access should be issued. This means that following the site keying hierarchy, if access is only required to a certain area or door, only a key for that area or door should be issued instead of issuing a sub-master or master key.

7.0 POLICIES INVOLVING CORPORATE SECURITY

Listed below are policies that have security considerations, where Corporate Security is an active participant.

7.1 Security Video Surveillance Policy

The "Security Video Surveillance Policy" was adopted by City Council in 2006 and follows the Information Privacy Commissioner of Ontario's "Guidelines for Using Video Surveillance Cameras in Public Places. Selected statements from the Policy include:

"*The City of Toronto (the City) recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of City employees, clients, visitors and property. While video surveillance cameras are installed for safety and security reasons, the City's video surveillance systems must also be designed to minimize privacy intrusion. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep City facilities and properties operating in a safe, secure, and privacy protective manner*.

The Security Video Surveillance Policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices at City owned and leased properties that are used for security purposes.

All City Staff must adhere to the video surveillance policy and must not access or use information contained in the video surveillance system, its components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.

No security video surveillance camera or system may be procured, installed, moved, altered, replaced, or erected without the approval of Corporate Security and only after following the procedures outlined in the Security Video Surveillance Policy."

As detailed in the Security Video Surveillance Policy "*a breach of this policy by an employee may result in discipline up to and including dismissal*."

The complete Policy can be found on the City's intranet. It is imperative that all staff are aware of the Policy and its obligations. As part of the on-going implementation of the Policy there are requirements to notify the applicable Unions and the Corporate Access & Privacy Office prior to the installation, relocation, or removal of a security camera. It is imperative that Corporate Security be immediately notified if a camera becomes out of service for any reason or a camera must be taken out of service due to construction, etc. This policy can be found on the City's intranet, on the Security & Life Safety site:
http://insideto.toronto.ca/fred/security_safety/index.htm
Link to Policy on Public web site: Toronto Security Video Surveillance Policy

7.2 Bomb Threat & Suspicious Package Response Policy

This document provides general training on bomb threats, including information on searches, evacuations, and detailed procedures to be followed when an employee receives a bomb threat. Since there is a greater chance of an explosive or other device being placed without some type of warning, this document also provides general training on suspicious packages and detailed procedures on what to do when an individual encounters a suspicious package.

This document can be found on the City's intranet, on the Security & Life Safety site:
http://insideto.toronto.ca/fred/security_safety/index.htm
Link to Policy on Public web site: Bomb Threat Procedures

7.3 Lockdown Procedures

Lockdown Procedures are defined in the Violence in the Workplace Prevention Guide (Canadian Centre for Occupational Health and Safety) as meaning "*… the people in a building take refuge in a secure location, e.g. in offices or classrooms. Lockdown procedures are usually initiated when it is unsafe to evacuate the building*."

The City's "Workplace Violence Policy" requires divisions to conduct workplace violence hazard assessments to determine whether the nature of the work or the work environment places, or may place, employees at risk of violence and to take all reasonable and practical measures to minimize or eliminate risks identified through the hazard assessment process, workplace inspections, or the occurrence of an incident.

Certain risk factors may be identified during workplace violence risk assessments that would separately or in combination warrant the development and implementation of lockdown procedures for a facility or group of facilities. Such risk factors may include:

- past occurrences at the facility or similar type of facility;
- past occurrences at neighboring facilities;
- proximity of the facility to potentially risk areas (schools, courts, etc); and,
- advice of the Toronto Police Service.

A document, "Guidelines for the Development of Lockdown Procedures" (was created as an appendix to the "Workplace Violence Policy" to assist divisions in creating Lockdown Procedures. Each division is responsible to determine whether a Lockdown Procedure is required and for which facilities. Corporate Security can assist divisions or facilities in reviewing these Lockdown Procedures.

7.4 Workplace Violence Policy

The City of Toronto is committed to working with its employees to provide a safe work environment. The City will not tolerate any acts of violence and will take all reasonable and practical measures to prevent violence and protect employees from acts of violence. Appropriate remedial, disciplinary, and/or legal action will be taken according to the circumstances.

For the purpose of the "Workplace Violence Policy", violence includes but is not limited to:

- Physical acts (e.g., hitting, shoving, pushing, kicking, sexual assault).
- Any threat, behaviour or action which is interpreted to carry the potential to harm or endanger the safety of others, result in an act of aggression, or destroy or damage property.
- Disruptive behaviour that is not appropriate to the work environment (e.g., yelling, swearing).

Some areas of the policy naming Corporate Security include:

"*Responsibilities:*
All employees are responsible for preventing and reporting acts of violence that threaten or perceive to threaten a safe work environment.

Management Staff of Divisions will:

- *Consult with Joint Health & Safety Committees (JHSCs), assigned Human Resources health & safety consultants, and where appropriate, Corporate Security, in conducting hazard assessments, and develop practical steps to minimize or eliminate identified risks*
- *Ensure that all known incidents of workplace violence are investigated and to the extent appropriate based on the nature of each incident and the actual or potential threat it posed to worker safety:*
    - *consult with other parties (e.g., Corporate Security, Health & Safety consultants, JHSCs, Employee Assistance, Human Rights office, Toronto Police Services).*"

The Workplace Violence Policy can be found on the Occupational Health and Safety page of the City's intranet under "Policies and Guidelines":
http://insideto.toronto.ca/hrweb/health_and_safety/index.htm
Link to Policy on Public web site: Work Place Violence Policy

8.0 CITY POLICIES WITH SECURITY CONSIDERATIONS

Listed below are policies that have security considerations, but contain parts that are, or are completely, out of scope for Corporate Security. These are policies that each employee should review and ensure they are compliant with when performing applicable work. All policies referenced can be found on the City's intranet.

These policies do not include Provincial Codes which also have sections that address security such as the *Ontario Building Code* and the *Ontario Fire Code*.

8.1 Maintenance Standards

Technical maintenance standards at corporate facilities were developed according to a recommendation of the Budget Advisory Committee. The Facilities & Real Estate Division worked with various divisions to ensure the standards met the varied needs.

The approved Maintenance Standards state that it is the responsibility of the various divisions and Agencies, Boards and Commissions to ensure the standards are carried out on buildings they're responsible for or arranged centrally through Facilities & Real Estate on a charge-back basis. The document provides maintenance standards which would be applied primarily to non-program facilities.

Section 5.5 of the document, "Security System Maintenance", details required preventative and on-going demand maintenance required for various security system components to ensure optimal functionality and prolong life span.

The "Maintenance Standards - City Facilities" can be found on the City's Intranet in the Facilities & Real Estate's division site:
http://insideto.toronto.ca/fred/operations/standards.htm

Link to policy on public web site: Maintenance Standards

8.2 Fleet Safety Policy

Sections of the City of Toronto's "Fleet Safety Policy" address theft of fleet vehicles, equipment, parts, or accessories. The "Fleet Safety Policy" can be found on the City's Intranet in the Fleet Services' division site:
http://insideto.toronto.ca/fleet/pdf/fleet_safety_policy.pdf
Link to policy on public web site: Fleet Safety

8.3 Fraud Prevention Policy

Areas covered under the "Fraud Prevention Policy" are under the purview of the Auditor General and not Corporate Security.

Any employee who has knowledge of an occurrence of irregular conduct, or has reason to suspect that a fraud has occurred, shall immediately notify his/her supervisor. If the employee has reason to believe that the employee's supervisor may be involved, the employee shall immediately notify the Auditor General.

The “Fraud Prevention Policy” can be found on the City’s Intranet in the Auditor General’s site:
http://www.toronto.ca/audit/fraud_policy_page.htm

8.4 Accessibility Design Guidelines

In June 2000, Toronto City Council adopted a motion to make the City fully accessible by the year 2008. In October 2000, Council requested that staff develop new accessibility design guidelines and start an audit of all City-owned buildings. City Council’s recommendation resulted in the preparation of the City of Toronto’s “Accessibility Design Guidelines”.

The major objective of the City of Toronto’s “Accessibility Design Guidelines”, which are based on Universal Design principles, is to provide practical examples of solutions that optimize accessibility to buildings and other buildings owned or occupied by the City of Toronto.

The guideline document is intended to guide City staff when considering or developing capital projects. The guidelines are in keeping with the Official Plan which states that "*A key city-building principle is that public buildings, parks and open spaces should be open and accessible to all members of the public including people with disabilities.*"

There are particular references to security and implications for security design contained in a number of sections in the guideline. The “Accessibility Design Guidelines” can be found on the City’s Intranet in the Diversity Management and Community Engagement site:
http://www.toronto.ca/diversity/accessibility_design_guidelines.htm

8.5 Graffiti By-Law

Graffiti poses a number of problems including:

- posing a risk to the health, safety and welfare of a community;
- promoting a perception in the community that laws protecting public and private property can be disregarded with impunity;
- fostering a sense of disrespect for private property that may result in increasing crime, community degradation and urban blight; and,
- creating a nuisance that can adversely affect property values, business opportunities and the enjoyment of community life.

The City of Toronto has introduced a “Graffiti Bylaw” (Municipal Code, Chapter 485) to guide City staff in preventing and enforcing the removal of graffiti effectively and immediately. Graffiti is defined in the “Graffiti Bylaw” as: "*One or more letters, symbols, figures, etching, scratches, inscriptions, stains, or other markings that disfigure or deface a structure or thing, howsoever made or otherwise affixed on the structure or thing, but, for greater certainty, does not include an art mural*".

City staff must remove graffiti on City-owned buildings, overpasses, bridges, and public parks. Staff will try to quickly remove any hate or gang-related graffiti within a 24-hour period and all other graffiti within a 72-hour period to prevent further proliferation.

Corporate Security Involvement

Corporate Security should be notified of graffiti on City buildings to ensure the graffiti is appropriately documented and the Police are notified. Corporate Security can be contacted though the Corporate Security Control Centre at 416-397-0000.

8.6 Corporate Access and Privacy Policies

The Corporate Access and Privacy Office of the City of Toronto administers a number of policies and guidelines that involve the protection of personal and confidential information at the City. These policies and guidelines can be found in the “Policies and Forms” section of the Corporate Access & Privacy Office website:
http://insideto.toronto.ca/cap/index.htm

Some of these applicable policies or forms include:

a) The "Clean Desk Policy and Guidelines"

The term "Clean Desk Policy" refers to workplace practices for employees to follow to keep paper and electronic records secure and prevent unauthorized access.

b) "Disclosure of Personal Information in Response to a Law Enforcement Request Form"

The Corporate Access and Privacy Office has developed a corporate "Law Enforcement Request Form" and guidelines to assist City staff in identifying when they are permitted to disclose personal information in response to a request received from a law enforcement agency in Canada, and specific procedures to follow when disclosing personal information in these circumstances.

c) "Guidelines for the Secure Use of Mobile Devices"

Mobile devices such as personal digital assistants (blackberries/PDAs), cellular phones and laptop computers present a unique set of privacy and security concerns. Theft includes both the hardware and perhaps most importantly, the loss or disclosure of sensitive personal and proprietary information. In an effort to mitigate this risk, the Corporate Access and Privacy office has developed guidelines to be used in conjunction with Corporate IT security policies and practices.

8.7 Municipal Code, Chapter 629 Property Standards

There are particular implications for security contained in a number of sub-sections of "Chapter 629, Property Standards".

9.0 APPLICABLE LEGISLATION AFFECTING SECURITY

The legislation below, while not a complete list, highlights sections of applicable Acts or Codes that provide a legislative action framework for, or are frequently used by, Corporate Security.

9.1 Private Security Guard and Investigators Act

The new *Private Security and Investigative Services Act, 2007*, was proclaimed on August 23, 2007. The new law requires security industry workers to be licensed, including some that were not licensed previously. Changes include standards for uniforms, equipment, vehicles, conduct, license eligibility, agency documentation/record keeping requirements, business registration, insurance, use of animals, term of validity and exemptions.

The purpose of this new Act is to strengthen the professional requirements for security guards and private investigators and to enhance public safety. This Act is overseen by the Ministry of Community Safety and Correctional Services, Private Security and Investigative Services Branch. Some important changes to the Act include:

Persons Who Perform Security Must Be Licensed

Under the Act, the definition of a security guard is "*a person who performs work, for remuneration, that consists primarily of guarding or patrolling for the purpose of protecting persons or property*." This means that individuals need a licence if they are paid to do work that consists mainly of protecting persons or property. The Act states that no person shall act as a private investigator or a security guard or hold himself or herself out as one unless the person holds the appropriate licence under this Act and is employed by a licensed business entity, a registered employer under the Act, or an employer that is not required to be registered.

Uniforms

In an effort to uniquely distinguish security guards and differentiate them from Police Officers, the act includes a regulation on uniforms that sets out requirements for shirt colour, hats, trouser stripes, identification tags, size and placement of words and logos, and rank chevrons. The Act states "*every person who is acting as a security guard or holding*

himself or herself out as one shall wear a uniform that complies with the regulations"

Vehicles

In an effort to uniquely distinguish marked security vehicles and differentiate them from Police vehicles, the act includes a regulation on vehicles. Under the new act, markings on security vehicles are not mandatory however, if a licensed business chooses to mark its vehicles, the regulation outlines the requirements that must be followed. The regulation sets out requirements governing size, placement and colour of words and logos, and prohibited markings.

Code of Conduct

The Code of Conduct outlines standards for the industry so that businesses and individuals know how to perform their duties in a professional, honest and respectful way. Discrimination and racism will not be tolerated, nor will negligence or unlawful conduct under the Code.

Security Guard License

The Act details that a "*Every person who is acting as a security guard or holding himself or herself out as one shall,*
(a) carry his or her licence;
(b) on request, identify himself or herself as a security guard; and
(c) on request, produce his or her licence."

Under the Act, Security Guards are required to produce their licence to a member of the public when requested. In the interest of public safety, members of the public have the right to know that they are dealing with a licensed security guard and/or private investigator. This means that the Security Guard must show the front of their licence to the individual, displaying the licence number, name and photo. Security Guards are not required to hand over their licence to a member of the public or show the back of their licence.

Complaints

Under the Act, any individual may make a complaint to the Registrar alleging that a licensee has breached the Code of Conduct established under the regulations or alleging that a licensee has failed to comply with this Act or the regulations or has breached a condition of a licence. The complaint shall be in writing, signed by the complainant, and

filed with the Registrar within 90 days after the subject-matter that gives rise to the complaint or at a later date with the Registrar's consent. The Registrar may, in writing, inform the licensee of the nature of the complaint.

Training and Testing

A new Training and Testing regulation is being drafted by the Ministry of Community Safety and Correctional Services.

The Training Curriculum will consist of:

1. Introduction to the Security Industry
2. The Private Security and Investigative Services Act and Ministry Code of Conduct
3. Basic Security Procedures
4. Report Writing
5. Health and Safety
6. Emergency Response Preparation
7. Canadian Legal System
8. Legal Authorities
9. Effective Communications
10. Sensitivity Training
11. Use of Force Theory
12. First Aid & Cardiopulmonary Resuscitation (CPR)

Licensees expected to be issued defensive equipment such as batons, handcuffs etc. will be required to take additional Specialized Training. Specialized Training on use of force will be required to be re-qualified annually or bi-annually.

9.1.1 Implications for the City of Toronto

The Act now requires businesses with in-house Security to have their in-house security personnel licensed. All City of Toronto Security (Guards) or other City positions that consists primarily of guarding or patrolling for the purpose of protecting persons or property, are considered in-house Security and are subject to the Act.

Under the Act, the City of Toronto had to register as an employer in accordance with the prescribed requirements.

Some of the changes will be phased in. The insurance and registration requirements came into effect on August 23, 2008; however, a two-year transition period will be provided for the uniform and vehicle regulations (August 23, 2009).

9.2 Criminal Code of Canada

There are a number of sections of the "Criminal Code of Canada" that effect Security personnel. Listed below are some relevant sections regarding the authority to arrest persons in certain circumstances, as well as, the authority to remove a trespasser.

Section 494 (1) Arrest Without Warrant By Any Person

"*Any one may arrest without warrant*

(a) a person whom he finds committing an indictable offence; or

(b) person who, on reasonable grounds, he believes

(i) has committed a criminal offence, and

(ii) is escaping from and freshly pursued by persons who have lawful authority to arrest that person."

This is means that a Security Guard may arrest someone who they witness commit an offence described as an indictable offence or as one punishable by indictment (generally the more serious of offences and as such carry greater penalties).

This also means that a Security Guard may arrest someone who they believe has committed a criminal offence (an offence against the Criminal Code of Canada) and is escaping from and being freshly pursued by a Law Enforcement Officer.

Section 494(2) Arrest By Owner

"*Any one who is*

(a) the owner or a person in lawful possession of property, or

(b) a person authorized by the owner or by a person in lawful possession of property, may arrest without warrant a person whom he finds committing a criminal offence on or in relation to that property."

This means that a Security Guard may arrest someone who they find committing a criminal offence on or in relation to the City property they are protecting. This section of the *Criminal Code of Canada* provides more authority to the Security Guard as the Security Guard can arrest for any criminal offence and does not have to distinguish whether the offence is classified as indictable, summary conviction, or dual procedure offence.

In all cases, arrested person must be forthwith delivered to a peace officer (Delivery to A Peace Officer - sec. 494(3)).

Section 41 (1) Defence of house or real property

"*Every one who is in peaceable possession of a dwelling-house or real property, and every one lawfully assisting him or acting under his authority, is justified in using force to prevent any person from trespassing on the dwelling-house or real property, or to remove a trespasser therefrom, if he uses no more force than is necessary*."

This is means that a Security Guard may use force to prevent a person from trespassing or to remove a trespasser from City property.

Section 41 (2) Assault by trespasser

"*A trespasser who resists an attempt by a person who is in peaceable possession of a dwelling-house or real property, or a person lawfully assisting him or acting under his authority to prevent his entry or to remove him, shall be deemed to commit an assault without justification or provocation*."

This is means that any person who resists the attempt of a Security Guard from preventing a person from trespassing or to removing a trespasser from City property can be arrested for assault.

9.3 Trespass to Property Act

A key purpose of this Act (Revised Statutes Of Ontario, 1990, Chapter T.21) is to allow an occupier (owner) or a person authorized by the occupier of property (Security Guard) to control who has access to their property and what behaviour or activities are allowed.

In this Act:

"Occupier" includes,

(a) a person who is in physical possession of premises, or

(b) a person who has responsibility for and control over the condition of premises or the activities there carried on, or control over persons allowed to enter the premises.

"Premises" means lands and structures, or either of them, and includes,

(a) water,

(b) ships and vessels,

(c) trailers and portable structures designed or used for residence, business or shelter,

(d) trains, railway cars, vehicles and aircraft, except while in operation.

Trespass An Offence - Sec. 2(1)

"*Every person who is not acting under a right or authority conferred by law and who,*

(a) without the express permission of the occupier, the proof of which rests on the defendant,

(i) enters on premises when entry is prohibited under this Act, or

(ii) engages in an activity on premises when the activity is prohibited under this Act; or

(b) does not leave the premises immediately after he or she is directed to do so by the occupier of the premises or a person authorized by the occupier,

is guilty of an offence and on conviction is liable to a fine."

Arrest Without Warrant On Premises - Sec. 9(1)

"*A police officer, or the occupier of premises, or a person authorized by the occupier may arrest without warrant any person he or she believes on reasonable and probable grounds to be on the premises in contravention of section 2*."

Delivery To Police Officer - Sec. 9(2)

"*Where the person who makes an arrest under subsection (1) is not a police officer, he or she shall promptly call for the assistance of a police officer and give the person arrested into the custody of the police officer*."

The Trespass to Property Act is an important act for Security personnel as it allows for persons to be directed to leave the property, to be arrested for failing to leave the property, and to ban individuals from entering the property in the future.

10.0 STAKEHOLDERS / PARTNERS

All City Divisions, Sections, and Units shall promote security by sharing applicable information with Corporate Security such as threats, incidents, or other activity in order to help the City maintain a safe and secure workplace.

Certain Divisions or Units are listed in this section to highlight additional responsibilities as it relates to Corporate Security or general security issues. This is not intended to be an exhaustive list for of all City Divisions or Units and their interaction with Corporate Security.

10.1 Access and Privacy Office

Corporate Security will ensure that it's staff adhere to all relevant policies and procedures provided by the Corporate Access and Privacy (CAP) Office. Corporate Security will involve the CAP Office in those aspects of the Security Video Surveillance Policy that relate to the City's privacy obligations under the Municipal Freedom of Information and Protection of Privacy Act and as prescribed by the relevant sections of the Security Video Surveillance Policy.

10.2 Community Safety Secretariat

It is recognized that community outreach and social development are important factors in the goals of gaining acceptance, buy-in, and usage of security measures. Corporate Security will consult with the Community Safety Secretariat on certain security measures to determine possible outreach initiatives that would assist in the above mentioned goals.

10.3 Human Resources Division

Human Resources staff must ensure they are aware of the requirement to immediately notify Corporate Security when an individual has left the employments of the City to ensure:

- the individual's access card is immediately deactivated;
- the return of access cards; and
- the return of keys.

10.4 Information & Technology

The Information & Technology division of the City is responsible for all information security. The Corporate Security Unit will liaise with IT with regards to the technical aspects of the Corporate Security systems (e.g. upgrades, network requirements).

10.5 Insurance and Risk Management Unit

Corporate Security will work with the Insurance and Risk Management Unit to reduce certain losses through the sharing of information. This partnership involves ensuring all loses of City assets due to theft, reported to the Insurance and Risk Management Unit, are investigated by Corporate Security and a Security Incident Report is created. This partnership also involves on-going sharing of information to identify and analyze reported incidents, to determine applicable measures to reduce future loss, and to forecast risk areas where losses can be reduced.

10.6 Purchasing, Materials Management Division

The Purchasing and Materials Management Division (PMMD) shall ensure applicable Security policies are adhered to by:

- only processing security hardware and security staffing requests approved by Corporate Security; and,
- ensuring the PMMD website provides a link from its call documents to reference the “Workplace Violence Policy” and where applicable the “Security Video Surveillance Policy”.

10.7 Law Enforcement Agencies

It is recognized by Corporate Security that law enforcement agencies, including the Toronto Police Service, are important allies in protecting City assets. Corporate Security draws on the information, advice, and expertise of these law enforcement agencies.

Corporate Security will act as a liaison with law enforcement, including the Toronto Police Service, to further the security needs of City assets. This liaison includes the sharing of applicable information, providing applicable incident reports related to criminal activity, and participating in crime prevention initiatives.

11.0 ADDITIONAL STATEMENTS

11.1 Complaints Process

11.1.1 Complaints About Security Guards

There exists two processes for making a formal complaint about any Security Guard: 1) a complaint to the Manager, Security & Life Safety or 2) a complaint to The Private Security and Investigative Services Branch, Ministry of Community Safety and Correctional Services.

1) Complaint to the Manager, Security & Life Safety, City of Toronto

Any member of the public or City of Toronto employee can file a written complaint with the Manager, Security & Life Safety which will be promptly and properly investigated.

Manager, Security & Life Safety
Corporate Security
Main Floor
Toronto City Hall
100 Queen Street West
Toronto, ON
M5H 2N2

2) Complaint to the Private Security and Investigative Services Branch, Ministry of Community Safety and Correctional Services.

Under the "Private Security And Investigative Services Act", 2007, "*Public Complaints: Should a member of the public have a complaint about the conduct of a security guard, private investigator or a licensed security business, they may file a formal complaint with the registrar of the Private Security and Investigative Services Branch*."

All complaints filed with the registrar must be in writing, signed by the complainant and filed within 90 days of the incident/occurrence. The registrar is responsible for investigating all complaints that have merit and are made in good faith. For more information or to obtain a complaint form, see the contact information and website link

below.

The Private Security and Investigative Services Branch
777 Bay Street, 3rd Floor
Toronto, Ontario
M5G 2C8
Telephone (Toronto area): 416-212-1650 toll free: 1-866-767-7454
Fax: 416-326-0034
www.ontario.ca/private-security

Provided below is the relevant excerpt from the Act regarding complaints and investigations.

PART V
COMPLAINTS AND INVESTIGATIONS

COMPLAINTS

Complaint to Registrar

19. (1) The Registrar may receive a complaint from any person alleging that a licensee has breached the code of conduct established under the regulations or alleging that a licensee has failed to comply with this Act or the regulations or has breached a condition of a licence. 2005, c. 34, s. 19 (1).

Form of complaint

(2) A complaint shall be in writing, signed by the complainant, and filed with the Registrar within 90 days after the subject-matter that gives rise to the complaint arose or at a later date with the Registrar's consent. 2005, c. 34, s. 19 (2).

Registrar to inform

(3) The Registrar may, in writing, inform the licensee of the nature of the complaint. 2005, c. 34, s. 19 (3).

Registrar may decline

(4) The Registrar may decline to deal with a complaint related to a breach of the code of conduct if, in the Registrar's opinion, the complaint is frivolous, vexatious or not made in good faith. 2005, c. 34, s. 19 (4).

Notice

(5) If the Registrar declines to deal with a complaint under subsection (4), the Registrar shall give notice of the decision to the complainant and shall specify the reasons for the decision. 2005, c. 34, s. 19 (5).

Referral to facilitator

(6) Unless subsection (4) applies, and if in the opinion of the Registrar the complaint is in regard to a breach of the code of conduct established under the regulations, the Registrar shall refer the complaint to a facilitator, unless the complainant does not wish the matter to be referred. 2005, c. 34, s. 19 (6).

Rules for facilitations

(7) The Registrar may establish rules concerning facilitations under this section, and a facilitator shall comply with any applicable rules. 2005, c. 34, s. 19 (7).

Attendance

(8) A facilitation shall not take place without the participation of the complainant and the licensee must attend any meetings required by the facilitator. 2005, c. 34, s. 19 (8).

Facilitation

(9) The facilitator shall attempt to resolve the complaint, and at the end of the facilitation shall communicate to the Registrar the results of the facilitation and either,

(a) his or her decision to make no recommendation; or

(b) his or her recommendation that the Registrar require the licensee to take appropriate remedial instruction. 2005, c. 34, s. 19 (9).

Registrar to act

(10) Where the facilitator has made a recommendation under clause (9) (b), the Registrar shall act in accordance with the facilitator's recommendations by imposing the taking of the remedial instruction as a condition of the licence. 2005, c. 34, s. 19 (10).

Registrar's authority not affected

(11) This section does not prevent the Registrar from exercising his or her authority under any other provision of this Act in respect of a licensee against whom a complaint has been made, whether or not the Registrar has dealt with the complaint under this section. 2005, c. 34, s. 19 (11).

11.1.2 Complaints About Security Policy or Procedures

Internal or external complaints made about any security issue in general should be addressed to:

Manager, Security & Life Safety
Corporate Security
Main Floor
Toronto City Hall
100 Queen Street West
Toronto, ON
M5H 2N2

11.2 Access and Equity Hiring and Training

The City of Toronto has a vision statement on access, equity and diversity that was approved by City Council in 2003. The statement articulates the corporate value and vision that guide the City:

- The City of Toronto values the contributions made by all its people and believes that the diversity among its people has strengthened Toronto.
- The City recognizes the dignity and worth of all people, equitable treatment of communities and employees, unique status of the Aboriginal communities and their right to self-determination.
- To address the barriers of discrimination and disadvantage faced by human rights protected groups, the City will implement positive changes in its workforce and communities to achieve access and equality of outcomes for all residents and to create a harmonious environment free from discrimination, harassment and hate.

In 2008, City Council approved a People Plan which outlines the goals for the City:

- We will be a learning organization
- We will have safe and healthy workplaces
- We will attract and retain a skilled, high performing and diverse workforce
- We will have strong and effective leaders
- We will build a positive workplace culture

The People Plan recognizes that "attracting and retaining a highly skilled, high performing and diverse workforce that reflects its community will have a positive impact on employee productivity, organizational effectiveness and the delivery of highly effective programs and services to Toronto residents and visitors".

11.3 Civilian Oversight

The area of civilian oversight is normally attributed to Law Enforcement in a public policing function where these agencies have additional legislative powers and governance. Civilian oversight for private security is typically done through legislative bodies such as the *Private Security and Investigative Services Branch - Ministry of Community Safety and Correctional Services* and *Information / Privacy Commissioner of Ontario*.

The Corporate Security Unit's actions are not only governed by City legislation, city policies, and external legislation and bodies, but the City also has an Ombudsperson who will investigate citizen complaints about the City.

The City is committed to providing open, and accountable government to the people of Toronto. One of the ways this is done is by the City holding open meetings, publicizing agendas and reports, and encouraging the public to attend committee meetings.

In order for Corporate Security to display this accountability and to provide community outreach, the Corporate Security unit will provide a webpage on the city's external website. This webpage will reference and provide applicable links to security policies involving the public, such as the *Security Video Surveillance Policy*; will provide the details of how to file a complaint via the *Private Security and Investigative Services Branch, Ministry of Community Safety and Correctional Service;* and will list major initiatives being taken by Corporate Security that effect publicly accessible City facilities.

11.4 Environmental Design

Security based environmental design is most often referred to as Crime Prevention Through Environmental Design (C.P.T.E.D.)

CPTED is a pro-active crime prevention strategy utilized by planners, architects, police services, security professionals and everyday users of space. CPTED surmizes that the proper design and effective use of the built environment can lead to a reduction in the incidence and fear of crime and improve the quality of life. Emphasis is placed on the physical environment, productive use of space, and behavior of people to create environments that are absent of environmental cues that cause opportunities for crime to occur.

Applying CPTED starts by asking what is the designated purpose of the space, how is the space defined and how well does the physical design support the intended function? Only then, can effective design or problem solving begin.

There are four underlying CPTED concepts:

1. Natural Surveillance - Is the placement of physical features and/or activities, and people that maximizes natural visibility or observation.
2. Natural Access Control - Deters access to a target and creates a perception of risk to the offender.
3. Territorial Reinforcement - Defines clear borders of controlled space from public to semi-private to private, so that users of an area develop a sense of proprietorship over it.
4. Maintenance - Allows for the continued use of a space for its intended purpose.

Many staff of the Corporate Security Unit are trained and certified in various level of CPTED. CPTED shall be a consideration in physical security design, before adding security video surveillance, and while examining a site in the Threat Assessment stage.

City divisions / sections / units responsible for the design of City facilities and design of major facility construction and renovation projects shall have a review completed of the design to ensure the consideration of CPTED principles.

12.0 REFERENCES

The following documents or portions thereof listed below contain information, which may constitute foundational knowledge for use in this Policy or are provided as informational references. At the time of writing, the editions indicated were valid.

ANSI Publications

ANSI/BHMAA156.28, *Recommended Practice for Keying Systems*, 2000.

ANSI/BHMAA156.30, *High Security Cylinders*, 2003.

ASIS Commission on Standards and Guidelines, ASIS International.

Worldwide Headquarters USA, 1625 Prince Street, Alexandria, Virginia 22314-2818

ASIS Chief Security Officer Standard, 2008 Edition

ASIS Workplace Violence Prevention and Response Guideline

ASIS Threat Advisory System Response (TASR) Guideline, 2008 Edition

ASIS Private Security Officer Selection and Training Guideline

ASIS Information Asset Protection Guideline

ASIS General Security Risk Assessment Guideline

IESNA Publications.

Illuminating Engineering Society of North America, 120 Wall Street, Floor 17, New York, NY 10005.

Lighting Handbook, 9th edition, 2000.

NFPA Publications.

National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471

NFPA 730, *Guide for Premises Security*, 2008 edition

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, 2008 edition.

UL Publications.

Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096

ANSI/UL 294, *Standard for Access Control System Units*, 1999, revised 2005.

ANSI/UL 437, *Standard for Key Locks*, 2000, revised 2004.

UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*,

2001.

UL 2058, *High Security Electronic Locks*, 2005.

ANSI/UL 3044, *Standard for Surveillance Closed Circuit Television Equipment*, 1999.

U.S. Department of Defense.

Unified Facilities Criteria (UFC), Washington, D.C.

DoD Minimum Antiterrorism Standards for Buildings, July 2002

U.S. General Services Administration Public Buildings Service.

U.S. General Services Administration Public Buildings Service Office of the Chief Architect 1800 F Street, NW Washington, DC 20405

The Site Security Design Guide, June 2007

Protective Design and Security Implementation Guidelines, February 2008

Security Standards for Leased Spaces

Security Design Criteria for New Federal Office Buildings and Major Modernization Projects

U.S. Government Publications.

U.S. Government Printing Office, Washington, DC 20402

FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, 2003

FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*, 2004

FEMA 430, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*

FEMA 452, *A How-To Guide to Mitigate Potential Terrorist Attacks Against Building*, 2005

FEMA 459, *Incremental Protection for Existing Commercial Buildings from Terrorists Attack: Providing Protection to People and Buildings*

U.S. Department of Justice. *Vulnerability Assessment of Federal Facilities*, 1995.

Other

Crowe, Timothy, 2000. *Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts*, Stoneham, MA: Butterworth-Heinemann.

General Services Administration (GSA), 2000. Chapter 8, *Security Design, in Facility Standards for the Public Building Service* (PBS-P100), Washington, D.C., November.

General Services Administration (GSA), 2007. *The Site Security Design Guide*, Washington, D.C., June.

Suggestions for improvement or correction of this document are welcome. They should be sent to:

Manager, Security & Life Safety
Corporate Security
City of Toronto