



Title: Base Building Security Standard

1. Effective date: October 31, 2018

2. Authority

This standard is issued under the authority of the Assistant Deputy Minister (ADM), Real Property Services (RPS), Public Services and Procurement Canada (PSPC).

3. Context

This standard is to be read in conjunction with the Treasury Board (TB) *Policy on Government Security*, the PSPC *Departmental Security Program (051)* policy, and the TB *Operational Security Standard on Physical Security*.

Real Property Services is identified as a lead security agency within the Treasury Board *Policy on Government Security*. Specifically, RPS is responsible for providing services related to base building security with respect to the PSPC Real Property Program.

4. Scope

This standard applies to all buildings and assets where PSPC has a custodial or ownership responsibility. This includes Crown-owned and leased assets, multi-tenant buildings, and other PSPC assets such as, but not limited to, bridges, dams, heating plants, and PSPC-controlled underground infrastructure such as underground utilities, transportation, or waste disposal.

5. Purpose

This standard ensures the uniform and efficient implementation of base building security in all PSPC custodial, leased, and engineering assets (specific to bridges and dams), as well as infrastructure assets (including, but not limited to, heating plants and underground plumbing and hydro connections), in accordance with the minimum standards set out in applicable policies, codes and regulations.

The purpose of this standard is to ensure common base building security practices across the national portfolio and ensure the common implementation of base building threat and risk assessments.

This standard will be reviewed every two years to ensure that it remains up to date, and reflects the most current security posture of the Department.

6. Details

Base building security

RPS, PSPC provides its clients with base building security services (protection of the asset infrastructure, including structural, mechanical, electrical, and architectural) and must develop and implement risk-based security in its portfolio.

Base building security is made up of both mandatory and risk-based security controls. Mandatory controls are outlined in Annex A of this standard. As a primary function, base building security must:

- apply approaches to mitigate the impact to the building that arise from criminal and unauthorized activity, in order to maintain the integrity, functioning and value of the building asset, including its structure and its systems;
- apply controls to deter criminal and unauthorized activity on all custodial property in public zones, areas, and property under the responsibility of PSPC and not under a client occupancy instrument;
- apply controls to mitigate the impact of threats and risks to custodial assets arising from environmental conditions, climate change, and geographic location;
- monitor and protect PSPC owned and leased assets to support the continuity of government operations;
- establish an environment of continual operational readiness in support of business continuity plans;
- provide adequate detection and response capacity to respond to known or foreseeable threats to the crown owned and leased asset;
- support Government of Canada security requirements for real property, including appropriate security and emergency plans and arrangements in the event of increased threat or readiness situations;
- support other emergency plans and arrangements as prescribed by Government of Canada policies, directives, standards and lead agency responsibilities in the *TB Policy on Government Security*; and
- support the timely implementation of reasonable and risk-based additional tenant-funded security measures, as indicated in the client threat and risk assessment.

Hours of operation covered by this standard are the hours included in the occupancy instrument, and include only those measures required by the base building threat and risk assessment and other governing legislation. Additional requirements outside the base building threat and risk assessment and the occupancy-instrument-specified hours are not considered to be covered under base building.

Base building threat and risk assessment

Standard base building security controls and tenant-funded enhancements for base building areas are identified primarily by base building threat and risk assessments which must be undertaken for all real property assets. Threat and risk assessment (TRA) processes are

outlined in Annex B. New assets or renovations require a site security brief and/or a security design brief at the inception phase.

Security requirements for tenant space, including transition space and other tenant-funded enhancements, are provided to RPS by the tenant department in a threat and risk assessment and/or a security design brief. These tenant costs are assessed as outlined in Annex C.

As a minimum, base building threat and risk assessments will identify and recommend physical security controls, as well as guard services, and/or other monitoring activities and procedures for the general protection of a custodial asset. Controls must facilitate appropriate detection and response on a 24/7 basis unless otherwise specified by a threat and risk assessment.

Base building threat and risk assessments, site security briefs, and design briefs must follow a prescribed format developed and updated by RPS's Property and Facility Management service line to provide a common approach, and to support risk-based security management of all PSPC owned and leased assets.

Base building threat and risk assessments must be conducted on a five-year cycle or when:

- There is a possible change in the threat environment identified locally, by RPS, the departmental security officer (DSO), or the tenant;
- There are changes in tenant departments or their operations, and the existing threat and risk assessment is no longer applicable due to an increased threat profile;
- There are plans to integrate new technology or systems within the facility that may impact the physical security risks in the environment; or
- There is a change in status of the building or a significant renovation planned.

At the initial phases of selection, design, and procurement of custodial assets, a current threat and risk assessment, or a base building threat and risk assessment, must be available and, if required, a site survey (site brief) must be conducted. It should be noted that an assessment of risk is required prior to the implementation of security controls.

Building assets must be categorized by their attributes and the security risks associated with the building operations. The Property and Facility Management service line maintains a profile of all custodian facilities, and acts as the central repository for such information. Annex D gives further information on the categorization of buildings.

The Property and Facility Management service line must be engaged directly in all circumstances where infrastructure has a high asset value, is located in heightened security environments, has a high symbolic value, or houses critical services.

The Property and Facility Management service line obtains, reviews and assesses threats and other data from the Government of Canada and other closed sources. Consequently, all base building threat and risk assessments and surveys completed at the local level must be submitted to the Property and Facility Management service line for review. The Property and

Facility Management service line will return, as appropriate, recommendations for the inclusion of additional controls to mitigate risks impacting PSPC custodial facilities as a result of the tenant's operations or sensitive assets to be located at the site.

Transition areas such as loading docks and reception zones must be adequately established and be appropriate to operations. Where possible, a building's physical attributes are to be considered in security planning.

Security enhancements to support access control into tenant space, either in a reception zone, mail room, loading area or other access point, is a tenant-funded enhancement. In a multi-tenant building, the Property and Facility Management service line works with the responsible building authority on building-wide security issues. The responsible building authority is accountable for ensuring action is taken to ensure the overall security of the building, adhering to the base building minimums, and resolving tenant level issues.

Monitoring and compliance

Compliance with this standard is mandatory. Compliance will be monitored and reported on through the base building security program, which performs a national oversight and quality monitoring role, and includes:

- continuous auditing throughout the life cycle of base building security for buildings, with appropriate reporting, by using base-building-security-tailored audit tools;
- preparation of an annual report on base building security;
- annual reporting on the status of implementation of threat and risk assessment recommendations;
- completion of base building threat and risk assessments as part of the Building Management Plan (BMP) National Call Letter.

7. Definitions

Base building (*immeuble de base*)

All elements related to the construction of, and systems required for, the services and functions of a building. This includes structural elements, building exterior (roof, windows, cladding, exterior doors, etc.), electrical, heating, ventilation and air conditioning (HVAC), conveying systems, interior finishes in common areas, fire and life safety systems, and building controls. Excluded from the definition of base building are internal elements related to tenant mandate or improvements/fit-up such as finishes and construction within a tenant space.

Base building security as defined in Treasury Board's *Operational Security Standard on Physical Security (sécurité de l'immeuble de base selon la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor)*

Security safeguards provided by the custodian department to protect a facility but not the assets contained in the building. Basic building security provides a base or starting point for other security requirements (i.e. minimum and enhanced safeguards) to be added to protect the specific assets held by the institution.

Base building security controls (*contrôles de sécurité de l'immeuble de base*)

Security safeguards, either physical or procedural, designed to protect the custodial asset and to render an environment suitable to house general Government of Canada operations. They consider the value and symbolism of the asset, but are limited to providing security that assures general protection of the asset, deters crime and unauthorized activity, and provides a reasonable expectation of security to persons and property on or in base building areas of responsibility. They do not include security controls required by virtue of the tenant operations or associated safeguards.

Base building security risk matrix (*matrice des risques en matière de sécurité de l'immeuble de base*)

A security risk management methodology applied to the information received during a base building threat and risk assessment. It is designed to categorize assets, and identify factors potentially related to heightened risk to the custodial assets as a result of tenant operations, or other factors causing risk.

In the selection of tenants for a building, the matrix assists in aligning tenant security requirements with a building's attributes to maximize the ability to implement appropriate security controls, and minimize costly security upgrades.

Base building threat and risk assessment (*évaluation de la menace et des risques pour l'immeuble de base*)

A standard document that prescribes how to conduct threat and risk assessments specifically designed for base building, that support the protection of custodial assets and the implementation of this standard. It includes physical security checklists, and a list of documents and standardized questions to be submitted to the Property and Facility Management service line as part of evidence-based security risk management.

Climate change adaptation (*adaptation aux changements climatiques*)

Security adjustments made by the Department in order to deal with the effect of potential climate change, given the increased risk of occurrence of natural disasters, rising global temperature, and increased precipitation. Current risks related to building security include increased risk of floods, weather events that exceed current building design standards to mitigate, extended periods of heat overcoming current HVAC or causing foundation instability, and interruptions to municipal services such as water and power.

Collateral threats (*menace collatérale*)

Threats to the persons, assets, or facilities that are the result of a facility's proximity to infrastructure or areas that are under higher threat, and where the impact of attacks against that infrastructure may adversely impact it.

Consequential threats (*menace indirecte*)

Threats to the persons, assets, or facilities that are the result of any involvement by another organization present in the building with other groups or issues.

Custodial facilities (*installations dont le Ministère a la garde*)

All real property assets (buildings, infrastructure, and land) where the Minister of Public Services and Procurement Canada, under the *Federal Real Property and Federal Immovables Act* has the administration of real property, including those that are leased or Crown-owned.

Facility (*installation*)

Any space primarily used for the delivery of Government of Canada services. A facility includes the main structure, surrounding property, and outbuildings associated with the delivery of services, or that hold Government of Canada infrastructure used to deliver those services.

Mandatory requirements (*exigences obligatoires*)

All direction derived from authoritative sources, including but not limited to legislation, regulations, and Government of Canada policies with respect to minimum baselines. They are to be applied consistently throughout the facility, and remain in force at all times.

Security design brief (*énoncé de la conception de la sécurité*)

A document that describes the physical protection philosophy and concepts, as well as physical safeguards, for a facility that are to be integrated into design and construction. It is a requirement at the inception phase for new assets or renovations.

Security infrastructure protection for non-building assets (*protection de l'infrastructure de sécurité pour les biens autres que des immeubles*)

The Department's custodial responsibilities for designated heating plants, dams, bridges, and warehouses, which require a range of integrated security controls for base building security infrastructure protection.

Security posture (*posture de sécurité*)

The overall plan and approach taken by the Department to deter security breaches or unlawful activity. This includes all phases from planning to implementation, and is comprised of control measures, both physical and psychological, which protect the department from security threats.

Security site brief (*énoncé de sécurité du site*)

A document that describes the physical security attributes sought in a site during acquisition. It is a requirement at the inception phase for new assets or renovations.

Specific service agreement (SSA) (*convention particulière de services [CPS]*)

An internal PSPC contract between one service branch and another government department. It describes the work to be done and associated costs.

Tenant-funded base building security controls (*contrôles de sécurité de l'immeuble de base financés par le locataire*)

Additional security controls identified to mitigate risks to custodial assets, or government operations housed therein, that are present as a result of the tenant's presence, operations, or other activities.

8. References

Legislation:

- [Access to Information Act](#)
- [Canada Labour Code](#)
- [Canada Occupational Health and Safety Regulations](#)
- [Canadian Charter of Rights and Freedoms](#)
- [Canadian Human Rights Act](#)
- [Emergency Management Act](#)
- [Federal Real Property and Federal Immovables Act](#)
- [Financial Administration Act](#)
- [Library and Archives of Canada Act](#)
- [Privacy Act](#)
- [Public Service Employment Act](#)
- [Security of Information Act](#)

Treasury Board:

- [Access to Information, Policy on](#)
- [Departmental Security Management, Directive on](#)
- [Contracting Policy](#)
- [Government Security, Policy on](#)
- [Identity Management, Directive on](#)
- [Management of Information Technology, Policy on](#)
- [Management of Materiel, Policy on](#)
- [Management of Real Property, Policy on](#)
- [Management of Risk, Framework for the](#)
- [Occupational Safety and Health](#)
- [Operational Security Standard - Business Continuity Planning \(BCP\) Program](#)
- [Operational Security Standard: Management of Information Technology Security \(MITS\)](#)
- [Operational Security Standard on Physical Security](#)
- [Security Organization and Administration Standard](#)
- [Security and Contracting Management Standard](#)
- [Security Screening, Standard on](#)
- [Values and Ethics Code for the Public Sector](#)

Other documents:

- [Departmental Security Program \(051\)](#)
- [RCMP G1-005 – Preparation of Physical Security Briefs](#)
- [Departmental Operations Center \(DOC\) Integrated Communications Protocol](#)
- [Crime Prevention Through Environmental Design \(CPTED\)](#)
- [Technical Reference for Office Building Design](#)





9. Attachments

Annex A – Elements of Base Building Security and Mandatory Controls
Annex B – Application of Threat and Risk Assessment for Base Building Security
Annex C – Delineation of Funding Responsibilities
Annex D – Building Categorization

10. Enquiries

Enquiries about this standard can be directed to [SI SSGII SIB / RPS PFMSL BBS \(TPSGC/PWGSC\)](#) generic inbox.

Any proposed modifications should be done in consultation with the Property and Facility Management service line. Also, any interpretation questions related to security portions of this document should be referred to the Property and Facility Management service line.

Elements of Base Building Security and Mandatory Controls

Base building security elements

The following are generic base building security elements:

- substructure
- shell
- facility perimeter
- grounds
- reception area for visitors
- roof
- loading dock
- electrical and mechanical rooms and systems
- building automation control systems
- elevators and other conveyances
- public areas – lobbies, washrooms, food courts
- any systems contained or encapsulated within the ceiling plenum or within walls
- heating, ventilation and air conditioning (HVAC) systems
- parking lot or underground garage
- ground floor doors and windows
- alarm systems that secure any base building space or system, excluding tenant-owned systems
- closed-circuit television (CCTV) equipment
- fire and life safety systems
- lighting (exterior and common space interior)
- steam/hot water pipe tunnels
- air supply and exhaust tunnels
- ducts and shafts
- sanitary/storm sewer and water services
- electrical
- information technology (IT) service infrastructure

Base building security mandatory security safeguards:

The following are generic base building mandatory security safeguards; other items may be added. Base building security controls are grounded in application of risk management so as to achieve the goals of physical security. Determining the mandatory security safeguards for buildings is the result of continuous review and evaluation.

- The facility is to have a clearly defined perimeter that indicates primary ownership and that control of the space is under the Government of Canada. Specific signage and perimeter controls will be determined as part of the recommendation of a threat and risk assessment, and take into account collateral and consequential threats. This applies to both whole buildings, and sections of buildings where PSPC is the custodian or leaseholder.
- Landscape design should support protection of the building, detection of intruders, and response to security incidents. It should employ the principles of Crime Prevention Through Environmental Design (CPTED) which can be found in the References section of the Base Building Security Standard.
- Lighting must provide sufficient illumination in and around the building to allow detection and observation of people approaching the building, and to deter criminal activity. Lighting plans and controls must be done in conjunction with any monitoring or surveillance equipment such as closed-circuit television equipment. With respect to CCTV equipment, the *Canada Labour Code*, *Canada Occupational Health and Safety Regulations*, and the lease, all indicate minimum lux levels, and should be referenced where applicable.
- Appropriate access controls that prevent unauthorized entry must be in place in all areas of the building to ensure that critical support systems are not tampered or interfered with. Examples of such controls are integrated electronic devices such as alarms and closed-circuit television equipment, and physical devices such as barriers, locks, doors, and specifically-designed integrated security controls for access points such as roof tops, loading docks, electrical and mechanical rooms, parking lots or underground garages, and ground floor doors and windows.
- A trained guard force, provided with current post orders for the specific facility or equivalent measures to provide detection and response capability for the facility as prescribed by a threat and risk assessment, is in place.
- Security monitoring of the building is done by means of alarm systems and closed-circuit television equipment which are monitored 24/7 by a security control centre, or equivalent measure as prescribed by a threat and risk assessment, to prevent unauthorized access to the building, especially during non-business hours.
- Security incidents which result in public property loss or damage, compromise the security of the asset, and/or involve criminal activity, workplace violence, or other criteria prescribed by the Property and Facility Management service line are reported through the appropriate channel.


Application of Threat and Risk Assessment for Base Building Security

The following are the key considerations for threat and risk assessments:¹

- **Purpose:** A threat and risk assessment is a process for evaluating specific threats to a building and infrastructure, determining the level of risk of the threats, and making recommendations to mitigate these threats.
- **Policy authority for threat and risk assessments:** The TB *Policy on Government Security* states that government wide threats and risks must be managed proactively. PSPC uses security practitioners to achieve this by completing up-to-date threat and risk assessments, as mentioned in the TB *Directive on Departmental Security Management*. The threat and risk assessment process is also an integral part of demonstrating due diligence under several laws and regulations pertaining to performance-based regulation, and is further supported in TB policy as being the foundation for any security controls or baselines.
- **Role:** The Property and Facility Management service line has the responsibility for developing the methodology and templates for threat and risk assessments, whether conducted by a third party or by Property and Facility Management service line staff. The Property and Facility Management service line monitors the program and ensures threat and risk assessments are conducted for all assets, which are updated as required, and by qualified persons, either through Property and Facility Management service line personnel or qualified third parties.
- **Application:** The Property and Facility Management service line provides approved threat and risk assessment methodology and templates under the supervision, review and approval of Property and Facility Management service line staff who are responsible for the final recommendations.
- If recommendations are altered or declined, the senior manager may request the intervention of the asset manager.
- If the risk is deemed unacceptable by the Property and Facility Management service line, or if the risk impacts a third party, a departmental security officer risk mitigation may be requested, or the risk acceptance may be forwarded for discussion between the DSO and the Director General, Service Lead, Property and Facility Management, RPS, or equivalent executive who is accountable for the custodial asset.

Note: Some threat and risk assessment recommendations or observations may, by TB policy or other legislation, fall under the lead tenant or other building occupant. In these cases, an extract from the threat and risk assessment containing the recommendations and references will be forwarded to the senior officer of the department in the building, and a

¹ *While a threat and risk assessment is a major tool for base building security, it should not be viewed as the only tool available. Constant review and challenge of the in-place security with ongoing discussion through the National Quality Monitoring, Maintenance Management and Security (NQMMS) team will help resolve specific building-level issues outside the base building threat and risk assessment process.*



copy sent to the security organization of the department after consultation with the PFM of the asset. The PFM will be consulted on wording and relevance and also included on the communication to the client department.

Delineation of Funding Responsibilities

Funding disputes are to be resolved in a manner that ensures that public funds are used effectively and efficiently, understanding that the operations of one federal entity are not to be managed in a manner that puts other federal entities or the Government of Canada as a whole at increased risk.


The following aspects of base building security fall clearly within the scope of PSPC or its sub-organizations:

- The facility perimeter and grounds, with security controls as described earlier in this document. These security controls are limited to the protection of persons, assets and operations as required by law, and the protection of the facility itself as appropriate to general Government of Canada operations and at the Government-wide threat level.
- Outbuildings or infrastructure points outside of the building envelope that are not specifically allocated for the delivery of a tenant's services. For example, a storage building used to contain equipment for the maintenance of grounds would fall under PSPC, whereas a shed that was used to house assets specific to a service delivered by the tenant would be the responsibility of the tenant.
- The building envelope as designed for general Government of Canada operations and taking into account the baseline threat environment in addition to threats to personnel and structures known to be prevalent in the area. This is intended to pertain particularly to natural threats such as flooding, fires, etc.
- Security controls put in place in response to risks that are a result of collateral damage due to the location of the facility in proximity to higher threat infrastructure.
- Public zones, reception areas, and transition points as described in Section 6, Details, of the *Base Building Security Standard*, and as per the Government of Canada baseline threat environment and routine operations.

The following aspects of security fall clearly within the scope of the tenant:

- Security controls that are intended not to protect the structure, but to protect tenant's personnel, assets or operations;
- Security required is either specific to the tenant, or the tenant is identified as operating at a higher threat level. These may include military, law enforcement, regulatory enforcement, or federal entities that participate in operations or activities involving conflict higher than the Government of Canada general operations.
- Security controls which extend into base building security systems either physically, electronically or procedurally², where such controls act as an additional layer of defense with respect to the protection of tenant assets.
- Security controls associated with the controlled access of stairwells or vertical transportation infrastructure (elevators and escalators) for purposes of limiting access to tenant-controlled spaces, or measures associated with restricting access to tenant-

² *Procedurally could include additional guard force personnel.*



controlled spaces. Continuity of access for the maintenance of base building infrastructure that occupies space within those controlled spaces must be maintained at the tenants' cost.

Building Categorization

The concept of categorization of buildings will assist in the threat and risk assessment (TRA) process, and other activities involved in base building security operations. It is one of the tools promoting standardization of the Base Building Security Program as it contributes to reducing and delineating costs associated with security measures in real property assets and infrastructure. The levels defined below do not denote activities that are funded by PSPC, but are used to help define the risk of certain occupancies.

The following describe how buildings are categorized:

Level One - High Security Posture: National security and law enforcement facilities where the tenant departments and agencies assume responsibilities for base building security. The Property and Facility Management (PFM) service line provides advice and guidance on site selection and design. It should be a single-occupancy building.

Parliamentary Precinct offices and their support facilities are considered Level One - High Security Posture, because of their symbolic value to the nation, and the Property and Facility Management service line provides base building security for them as they are part of Public Services and Procurement Canada. The exceptions within the Parliamentary Precinct are the Centre, West and East Blocks where Parliamentary Protection Service (PPS) provides all of the security, including base building security.

Level Two - Medium Security Posture: National headquarters facility for departments and agencies with defined exterior perimeter and reception area covered by integrated security controls.

Level Three - Basic Security Posture: General offices with basic base building security to ensure a level of protection from criminal activity outside the building and in the public areas, as well as to ensure no unlawful access the building.

Level Four - Federally-Controlled Critical Infrastructure: Other buildings requiring a range of specific security controls, such as those for heating plants, dams, bridges and warehouses which are departmental assets under its custodial care. This also includes data storage centres managed by Shared Services Canada.

Note: Security provisions are required during any construction, renovation or refit to ensure that the security posture is maintained.

Table 1: Categorization of buildings and security regimes and building attributes

The concept of categorization of buildings is one of the tools promoting standardization of the Base Building Security Program, as it will contribute to reducing and delineating costs associated with security measures in real property.

CATEGORIZATION OF BUILDINGS AND SECURITY REGIMES AND BUILDING ATTRIBUTES		
Levels	Examples of key building attributes	Tenants' requirements
<p>Level One - High Security Posture</p>	<p>Types of organizations*:</p> <ul style="list-style-type: none"> • National security and law enforcement facilities • Parliamentary affairs (Parliamentary Precinct) • National security and/or intelligence organizations, or those organizations with significant information holdings impacting the national interest • Tenants whose operations may impact the security of other departments or organizations • Departments housing certain critical services or assets (such as server farms, etc.) <p>*As determined by a threat and risk assessment</p>	<p>Threat and risk assessments and security design briefs will provide recommendations that may include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Special care in site selection so that these organizations are not co-located next to or near to tenants who themselves have a high security risk profile (e.g. banks, Royal Canadian Mounted Police (RCMP)). • A physically-defined perimeter large enough to provide appropriate standoff space, controlled entrances and parking areas. May also require standoff space from neighbouring buildings in order to protect from electronic penetration. • Regional offices open to the public may require the same security provisions as the main office. • Smaller regional offices with limited visitor access in multi-tenant buildings may require specialized security provisions, in particular protection against electronic penetration.



		<ul style="list-style-type: none">• Increased security screening for employees at various levels at various hours.• Security controls to provide safety for staff offices, by means of controlled access for visitors and others on official business, as well as at loading docks and rooftop access points.• The application of ballistic- and bombproof structural capability, as well as reinforced entrance doors.• High-level access controls and high-level security controls built into support-facility design.• Ability for security posture to be heightened in periods of increased threat.• Enhanced security screening for all privately-owned amenity spaces within the facility.• The PFM service line provides advice and guidance on planning, site selection, and design for national security and law enforcement facilities.• Tenant may require ongoing integrated operational support from the PFM service line, or may provide its own security.• Tenant may require PSPC staff and contractors to have enhanced security screening after commissioning.
--	--	--



<p>Level Two - Medium Security Posture</p>	<p>Types of organizations:</p> <ul style="list-style-type: none"> • A departmental headquarters housing ministers / deputy ministers • An organization whose mandate and activities may impact the application of Base Building Security • An organization whose national threat assessment will impact the application of Base Building Security 	<p>Threat and risk assessments and security design briefs will provide recommendations that may include but are not limited to the following:</p> <ul style="list-style-type: none"> • May be located in a multi-tenant building which is largely government that may have some integration of private business Access controls by means of integrating electronic devices, such as alarms and CCTV, with locks and doors. • Continuous security monitoring 24/7 of access controls, and adequate response time to security incidents. • Support from a guard force controlled by base building, with post orders (written documents that outline duties, responsibilities and expectations of guards) delineating base building and tenant responsibilities. • May require clearly defined lead tenant roles and responsibilities. • Appropriate plans and arrangements to increase security of the whole facility under the control of the lead tenant and PSPC or third party provider. • May require screening of private businesses, and restriction of access during times of heightened security.
---	---	--

		<ul style="list-style-type: none"> • After-hours access may be limited to authorized personnel. • Parking may be controlled by the lead facility tenant. • Clearly-defined reception zones. • Ability for security posture to be heightened in periods of increased threat. • Parking elevators should open into a reception zone in the ground floor elevator lobby. • May require security screening at a level corresponding to the security level of information and assets in the building. • All employees that work in privately-owned amenity spaces within the secure perimeter may be required to have security status of reliability at a minimum. <p>Example: Terrasses de la Chaudière and Place du Portage</p>
<p>Level Three – Basic Security Posture</p>	<p>Types of organizations:</p> <ul style="list-style-type: none"> • General offices space in Crown owned or leased space. 	<p>Threat and risk assessments and security design briefs will provide recommendations that may include but are not limited to the following:</p> <p>General office space:</p> <ul style="list-style-type: none"> • Defined zones, with base building security centre of expertise providing advice and guidance for the public and reception areas, in co-



		<p>operation with the tenant's security requirements.</p> <ul style="list-style-type: none">• Ensure that access controls for the tenants' space are supported by a guard force so that there is 24/7 continuous monitoring, and there is an adequate response time to security incidents.• Security screening at the appropriate level corresponding to the security level of information and assets in the building.• Escorted maintenance personnel.• Ability for security posture to be heightened in periods of increased threat.• May require a Building Security Committee, and security incidents should be reported to National Base Building Security Centre of Expertise.• Parking elevators should open into a reception zone in the ground floor elevator lobby.• The base building security objective is to ensure protection from criminal activity outside the building and in the public areas, as well as to ensure there is no unauthorized access to the building.• Planning, design and site selection must include
--	--	---



		<p>base building security requirements.</p> <ul style="list-style-type: none"> • Leases and occupancy agreements must include all necessary security provisions. • If the tenant’s mandate and activities require additional security controls, these are implemented in the planning and design phase, or when there are changes in the security requirements. <p>Example: Constitution Square</p>
<p>Level Four - Federally-Controlled Critical Infrastructure</p>	<p>Types of facilities:</p> <ul style="list-style-type: none"> • Heating plants, dams, bridges and warehouses (assets under PSPC custodial care). • Data storage centres managed by Shared Services Canada. 	<p>When produced for federally-controlled critical infrastructure facilities, threat and risk assessments must be written using an all-hazard approach, and with the understanding that each type of facility requires specific security controls. They may include but are not limited to the following:</p> <ul style="list-style-type: none"> • Ability for security posture to be heightened in periods of increased threat. <p>These are critical infrastructure facilities where function, locality and the national threat assessment will impact on the department’s security posture for each type of facility.</p>