Physical Security Considerations in Facility Design

GCPSG-014 (2024)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2024-07-01
Updated: YYYY-MM-DD

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

This guide on Physical Security Considerations in Facility Design is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication to serve as a guide for developing physical security design briefs for departments, agencies and employees of the Government of Canada.

Suggestions for amendments and other information can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Effective Date

The effective date of GCPSG-014 (2024) – Physical Security Considerations in Facility Design is 2024-07-01

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

Note: Authority for modifications or variances is Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

Contents

1. Introduction

The RCMP, as the Lead Security Agency (LSA) for Physical Security for the Government of Canada (GC) is responsible for providing advice and guidance on all matters relating to physical security.

1.1. Purpose

The purpose of this document is to provide Government of Canada (GC) security personnel with guidance on the preparation of physical security design briefs and associated components and considerations for GC facilities; whether new construction or retrofit of existing spaces. This guide should be used in conjunction with a Threat and Risk Assessment (TRA) and/or Threat-Based Design to determine specific needs. Specific technical details about security equipment are not discussed in this guide (such as types of door hardware or intrusion alarms).

This guide is intended to be used in conjunction with other published RCMP LSA guides which are available at Lead Security Agency for Physical Security - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

1.2. Applicability

This guide is applicable for GC employees with the responsibility of the design, construction, or renovation of a GC building or facility. Additionally, this guide applies to security personnel assigned with the development of physical security design briefs to ensure relevant physical security considerations and standards are reported to the project manager and are built into the project at the earliest possible phase.

1.3. Equity, Diversity, and Inclusion in Physical Security Systems

All employees of the Government of Canada (GC) have a responsibility to safeguard persons, information and assets of the GC. It is important that security policies and practices do not serve as barriers to inclusivity, but instead support and respect all GC personnel while ensuring appropriate security measures are maintained for the protection of GC personnel, assets, and information.

Initiatives to promote equality and inclusion among the diverse communities and heritages within the GC, should be respected in the development and maintenance of physical security systems. Departments and agencies should follow all GC legislation, policy and directives on Equity, Diversity, and Inclusion (EDI) in the promotion of a fair and equitable work environment for all persons while ensuring they meet their mandated security responsibilities.

Departments and agencies should conduct a risk management exercise to ensure, that while the dignity of all is respected, the protection of GC information, assets, and personnel is

maintained. All questions on EDI policies and directives should first be addressed to your responsible departmental authority.

1.4. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in Government of Canada controlled buildings is critical. Some examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC, etc.

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components of the applications and/or software controls are maintained and that any risks highlighted will be mitigated. Starting the SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental Security.

2. Contact Information

For more information, please contact:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronyms

Acronym	Meaning
CCTV	Closed Circuit Television – includes related video equipment
CPTED	Crime Prevention Through Environmental Design
EID	Electronic Intrusion Detection
FSA&A	Facility Security Authorization and Assessment
HSZ	High Security Zone
GC	Government of Canada
OZ	Operations Zone
PGS	Policy on Government Security
PZ	Public Zone
RAA	Restricted Access Area
RCMP LSA	RCMP Lead Security Agency for Physical Security

RZ	Reception Zone
SA&A	Security Assessment and Authorization
SDB	Security Design Brief
SOC	Security Operations Centre
SZ	Security Zone
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment

4. Glossary

Term	Definition
Closed Circuit Television (CCTV)	Any electronic surveillance system consisting of cameras, monitors, recording equipment, and other technologies to monitor any space. Interchangeable with CCVE.
Compartmentalization	The physical separation of an area(s) within a structure
Facility Security Assessment and Authorization (FSA&A)	A process by which organizations ensure that security assessments are performed on new and existing GC facilities and fit-up projects. Appropriate security controls are identified and implemented before authorization is given to allow the facility to be occupied.
Glazing	Transparent material used for windows
High Security Zone (HSZ)	An area where access is limited to authorized personnel holding the corresponding GC Security Clearance and to pre-approved/screened, properly escorted visitors. Example – area where information and assets classified higher than Secret are processed or stored.
Operations Zone (OZ)	An area where access is limited to personnel who work within and to properly escorted visitors only. Example – Government office space/staff only warehouse
Public Zone (PZ)	An area where the public has unimpeded access and generally surrounds or forms a portion of a government facility. Example – grounds surrounding a building.
Reception Zone (RZ)	An Area where the transition from a Public Zone to a restricted-access area is controlled. Example – Reception lobby or Security Guard Post
Restricted Access Area (RAA)	A work area (site or building) within a department/agency where access is limited to authorized individuals. This includes Operations Zone, Security Zone, and High Security Zones as defined in GCPSG-015 Guide to the Application of Physical Security Zones
Security Design Brief	A document which describes the physical protection philosophy and concepts as well as physical safeguards for a facility.
Security Zone (SZ)	An area to which access is limited to authorized personnel holding the corresponding GC Security Clearance and to properly escorted

	visitors. Example – area where information classified up to and including Secret is processed or stored.
Stand-off	The distance between a potential threat and the asset. Example – Public street (public zone) to entrance of a building (reception zone)
Threat	Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.
Threat-Based Design	Applying preventative measures and safeguards into the design of a building, facility, or space. Based on principles found in the International Atomic Energy Agency's *Design Basis Threat.*
Threat Risk Assessment (TRA)	Assessment of a facility to identify risk, threats and vulnerabilities to assets (information, employees, services, etc.).
Unauthorized Access	Access to information or assets by an individual who is not properly security screened and/or does not have a "need-to-know".

5. Assessing Physical Security Needs

In order for a physical security system to be effective, it must be developed based on an understanding of the threats and risks it is designed to control. Specific technical details about security equipment are not discussed in this guide (such as types of door hardware or intrusion alarms); however, methodologies for incorporating physical security systems into the design of a building or facility, as opposed to adding these systems afterwards, are highlighted. This approach can be accomplished through the use of the following concepts and/or activities. Information obtained or used in the facility design process that is classified in nature may need to be classified in accordance with Directive on Security Management standards and handled in accordance with GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material.

5.1. Threat and Risk Assessment

Threat and Risk Assessment (TRA) is a process used to identify, analyze, and address observed vulnerabilities against known or anticipated threats, to establish the risk environment, and is an integral part of a department or agency's overall risk management strategy. TRAs vary in scope and application but this process can enable greater efficiency in identifying and resolving vulnerabilities throughout the entirety of a construction project. The RCMP LSA can provide additional information on the TRA process in GCPSG-022 (2024) Threat and Risk Assessment Guide or by contacting RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

5.2. Threat-Based Design

Threat-Based Design is a profile of the type, composition, capabilities, methods, projected harm, and/or intensity of a deliberate, accidental, or natural threat upon which the security engineering and operations of a facility is based. This is based on principles found in the International Atomic Energy Agency's Design Basis Threat. Threat-based design is intended to eliminate or reduce the impact of threats attributed to vulnerabilities in the design or

location of a facility; thus, both threat-based design and TRA should be used in tandem. The steps in Threat-Based Design are:

5.2.1. Threat Assessment

The Threat Assessment phase of threat-based design requires the gathering of all relevant information for a preliminary assessment of the threats requiring mitigation measures incorporated into the design of a building, facility, or space. Information gathered during a TRA may be included in this phase as it supports the same purpose.

5.2.2. Information Gathering

The information-gathering process is intended to identify and list potential threats to the proposed facility. Often identified during a TRA, this may include threat motivation, intention, capability, and historical occurrences. Reliable sources of information should be consulted, including intelligence and law enforcement agencies, government departments and agencies, incident reports, as well as historic and current TRAs and other relevant risk assessments. The credibility of the information, and the information source, should be assessed in the same manner as a TRA. Information gathering should be a continuous activity throughout the lifecycle of a threat-based design list to confirm the information remains relevant and reflects the most up-to-date data.

5.2.3. Preliminary Analysis

The information obtained is then analyzed to document credible motives, intentions, and capabilities of potential threats. The analysis should pay particular attention to potential threats that are relevant and realistic to the department or agency's mandate and the location of the facility. The aim of this phase is to provide a credible assessment of potential threats, including composition, motivation, intention, and capabilities.

The following attributes of each threat should be considered in the analysis; however, there may not be data available due to lack of information or lack of credible information for each threat:

- Motivation
- Intentions
- Tools
- Technical Skills
- Cyber Skills
- Knowledge
- Funding
- Insider Threat
- Tactics
- Complexity
- Frequency of historic events
- Attractiveness of Target

The product of this phase is a threat assessment document that describes the threat environment and all known threats to be taken into consideration. As previously noted, information from a TRA may be used in the development of the threat-based design document.

5.2.4. Secondary Analysis

The threat assessment document is then analyzed based on the available attributes. The relevance of each threat can be determined based on the motivation, intention, and/or capability to harm. Threats with higher relevance should be taken with higher consideration compared to those with less relevance. Threats with similar attributes can be assigned into threat types defined by specific attributes and characteristics. Considerations to include in the larger threat types can be specific site and activity considerations; such as operational procedures at the facility, location and accessibility of the facility, and transportation modes/routes to and from the facility. The information analyzed is then compiled into a document outlining an overview of the threat, as well as its attributes and characteristics relating to the facility.

The results of this document as well as the TRA can be used to develop the security design brief for the facility.

5.3. Security Design Brief

The content of a Security Design Brief (SDB) will vary, depending on whether the department or agency is leasing existing facilities or constructing new GC-owned facilities. The level of detail normally provided in an SDB is general in nature; in order to provide maximum flexibility in the design process. The elements of a facility listed under Section 6. Physical Security Considerations in Building Design and Section 7. Safeguards are a selection of factors that should be included in any SDB. Additionally, these elements may have an interdependent relationship that should be highlighted, to reinforce the value of incorporating safeguards that may address multiple vulnerabilities or threats.

It is beneficial to cross-reference, or note, the recommendations of the TRA or threat-based design documents to the applicable recommendations in the SDB; as these are the corrective measures intended to minimize the vulnerability and risks reported in those processes. The SDB should begin with an introduction and purpose, followed by applicable design considerations and safeguards, and should conclude with any references and supporting documentation (such as the TRA and Threat-Based Design documents). Once completed, the SDB should be provided to the project manager and other relevant personnel.

Depending on the facility, there may be additional design considerations and/or safeguards that are not included in these aforementioned sections of this guide. It is up to the department or agency to determine, based on its findings from the facility's TRA and/or

threat-based design document, what measures are required for a given facility and develop recommendations to remove or minimize vulnerabilities in the facility's design and construction.

5.4. Facility Security Assessment and Authorization Process

Facility Security Assessment and Authorization (FSA&A) is a process by which organizations ensure that security assessments are performed on new and existing GC facilities and fit-up projects. The FSA&A process consists of five (5) phases:

- Initiation;
- Planning;
- Risk and Analysis;
- Implementation, Authorization and Ongoing Security Assessments, and;
- Decommissioning.

TRAs, Threat-Based Design, and SDBs each fit into one of the phases of the FSA&A process. TRA and Threat-Based Design takes place in the Risk and Analysis phase, after which the SDB is developed during the Implementation, Authorization, and Ongoing Security Assessments phase. For more information on the FSA&A process, please consult GCPSG-016 - Guide to the Facility Security Assessment and Authorization Process.

5.5. Management Summary

Due to the length of SDBs, TRAs, and Threat-Based Design documents, it is preferable to create a two (2) to three (3) page summary or briefing note, including supporting documentation, for project decision-makers. The management summary should only highlight the specific design concepts related to each major attribute listed in the brief. The intent is to assist senior managers in quickly capturing the important design ideas necessary for safeguarding the facility, as well as to enable a decision to proceed with the project.

6. Physical Security Considerations in Building Design

Whether constructing or retrofitting a facility, physical security should be considered during the design process. Results from a TRA and Threat Based Design will aid in determining specific requirements for a given facility which should then be addressed in the SDB. This section is intended to be used in conjunction with guidance from GCPSG-019 – Protection, Detection, Response, and Recovery Guide, GCPSG-015 – Application of Physical Security Zones Guide, GCPSG-006 - Access Management Guide, and other listed GCPSGs when compiling an SDB for a facility.

6.1. Protection, Detection, Response, and Recovery

Protection, Detection, Response, and Recovery is based on the principle that the external and internal area of government facilities can be designed and managed to create

conditions that, together with specific physical security control measures, will reduce the risk of harm to employees, protect against and detect unauthorized access or attempts to access, and activate effective response and recovery activities. For more information consult GCPSG-019 – Protection, Detection, Response, and Recovery Guide.

6.2. Physical Security Zones

Physical security zones, when appropriately integrated, should enhance the overall security environment of a facility. Physical security zoning should promote a sense of ownership or territorial reinforcement, provide opportunities for natural surveillance, and establish a clearly defined sequence of boundaries through which an appropriately screened visitor or employee may pass through. Departmental functional space requirements should also be taken into consideration when establishing zoning boundaries.

Physical security zoning should not be implemented by simply adhering to the prescribed technical requirements for zones nor by integrating zones into the plan based solely on functional space requirements. If physical security measures that demarcate zones are excessive, inappropriate, or have not considered the functional space requirements, these measures will eventually be bypassed and could become ineffective. Incentives for unauthorized personnel to cross zoning boundaries (such as washrooms or a cafeteria) should be avoided or removed.

Refer to GCPSG-015 Guide to the Application of Physical Security Zones for more information on zoning.

6.3. Perimeter of Building and Property

Stand-off distance is important when considering the site/building perimeter as it allows for early detection of a threat which in turn allows for quick response and limits damaging effects on staff and infrastructure. The exact distance can vary based on a variety of factors and a TRA can aid in determining an appropriate distance. This should be considered in both the construction and/or relocation of a facility.

Fencing can be used for the perimeter of the site. For more information consult GCPSG-009 Security Fencing Considerations Guide.

With the exception of easements, the facility may have to abut the property line, a street or the wall of an adjacent building on some sites. If separation from the property line cannot be achieved, more robust security features and procedures will be required. For more information consult GCPSG-019 – Protection, Detection, Response, and Recovery Guide.

6.4. Life Safety and Emergencies

While physical security measures are required, they must not supersede nor negate life safety measures or legal requirements. For example, Security Zones (SZ) and High Security

Zones (HSZ) still require the ability to exit in an emergency; therefore, emergency exit doors must still be equipped with panic bar hardware to expedite emergency egress. Refer to all applicable codes and policies including, but not limited to, the Canada Labour Code, National Fire Code of Canada, National Building Code of Canada, Provincial/Territorial/ Municipal codes, and relevant TBS policies to ensure compliance.

6.5. Location of Exit Stairwells

Exit stairwells which form part of a means of egress must comply with the National Building Code requirements. These stairwells should not allow any uncontrolled access to Operations Zone (OZ), SZ, or HSZ. Best practice is for doors in a SZ and HSZ to exit to a less restrictive zone prior to accessing a public space without exterior door hardware capable of granting access into the zone.

6.6. Elevators and Elevator Lobbies

Elevators, including freight/cargo elevators and dumbwaiters, should not allow access between zones. Elevators should only allow access between the same zones (Reception Zone to Reception Zone). Elevator lobbies, including freight/cargo elevators from public parking and loading docks, should open in a Public Zone (PZ) or Reception Zone (RZ) such as a ground floor elevator lobby to ensure only authorized, appropriately screened individuals are allowed access into a facility's space. Should the elevators open into an OZ, there is a greater possibility of unauthorized individuals accessing the GC space undetected.

6.7. Pedestrian Circulation Routes

Pedestrian circulation routes from PZ to OZ should pass through a RZ under the institution's control to ensure control of access; as per GCPSG-015 – Application of Physical Security Zones Guide. All stairs required as a means of egress for PZ should be located in the PZ.

Exit doors as a means of egress from restricted-access areas (RAA) to PZ should be equipped with automatic closers and secured on the stairwell or corridor side, with the exception of crossover floors in high-rise buildings. Signs on doors from higher-restriction zones should indicate one-way movement or other appropriate signage.

Any security measures that are used to compensate for site-specific deficiencies are to be included in SDB. Electronic access control can be used to regulate the movement of personnel around the facility.

6.8. Pedestrian Control Within a Building

Sufficient space should be provided in RZ to accommodate visitors waiting for service while not disrupting normal activity in the facility or on premises. Sufficient overflow space in PZ may also be used to ensure normal operations can continue in the event of a sudden influx of visitors. At the perimeter of the institution's space, there should be the potential to erect a physical or psychological barrier as a means of access control in a situation such as a protest

or shelter in place event. For more information, consult GCPSG-006 Access Management Guide.

6.9. Windows

Windows should follow architectural requirements with consideration on security and safety glazing included in the design phase of the project. Refer to GCPSG-013 Fundamentals of Glazing in Physical Security for more information and specifications.

6.10. Common Spaces

All common functions within the building should be located in centralized areas. These areas should be part of an OZ and could include, for example, lunch/coffee rooms, washrooms and general photocopy rooms. Common areas for visitors such as washrooms, interview rooms and orientation spaces should be located in the RZ. The intent is to reduce pedestrian movement into RAAs, and to eliminate reasons for persons not working in the RAAs to enter legitimately.

6.11. Washrooms

Public washrooms should be located where there is unobstructed visual observation of the entry by a receptionist or guard. Staff washrooms, if indicated in a TRA, can be located in an OZ. Staff washrooms should be separate from public washrooms for employee safety and to minimize the possibility of unauthorized access to any RAA.

6.12. Utility Spaces

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

Utility spaces should not be located adjacent to entrances to more restrictive zones. If possible, they can be located near intended access management locations such as guard screening areas.

6.13. Adjacent Occupants

Access to an institution’s space should be controlled. The impact of departmental operations on adjacent occupants should be considered. Likewise, the mandate and operations of adjacent occupants should also be taken into consideration in relation to departmental mandate and operations.

In a multi-tenant building with GC offices spanning several floors, elevator systems that separate floor access in the lobby can help prevent unauthorized access to GC space(s) depending on the elevator bank, access cards, and management of visitors by security personnel. For more information consult GCPSG-006 - Access Management Guide.

6.14. Telecommunications and Data Links Within the Facility

A TRA should be used to determine appropriate physical security measures for telecom wiring within a facility. Additional information can be found in the Policy on Service and Digital.

The need to implement protective measures within the facility, such as emergency power for the intercom or internal telephone and the routing of conduit to carry communications should be determined by the TRA and/or Threat-Based Design. For more information refer to Appendix C of GCPSG-015 (2023) - Guide to the Application of Physical Security Zones

6.15. Mailrooms

Mailrooms should be managed as an OZ at minimum. Mailrooms should be located in or near a shipping/receiving area separate from RAAs or critical infrastructure. They should be separate from RZs and have the capability to be isolated from the rest of the building in case of suspicious packages or other threats.

6.16. Loading Docks

Loading docks should be located away from and not directly linked or adjacent to RAAs or critical infrastructure components. While shipping and receiving areas can be located in the same loading dock, it is beneficial to physically separate the areas to limit the impact of a threat actor should they gain access.

6.17. Conference and Board Rooms

Conference and board rooms should be located in an OZ at minimum. If these spaces are to be used to discuss sensitive or classified information, they should be included in the design of the zones with additional sound attenuation and appropriate access management.

6.18. Computer and Server Rooms

Physical security as it pertains to computer server rooms is based on the implementation of positive control. Under positive control, a space or asset is actively monitored and continuously protected so that any change, or attempted change, to its status is immediately known. Computer and server rooms should be managed as RAAs, with best practice being limiting access to essential personnel only. For facilities housing classified servers, these RAAs must be located in a SZ. For more information refer to Appendix C of GCPSG-015 (2023) - Guide to the Application of Physical Security Zones.

6.19. Special Purpose Space

This document focuses on attributes associated with general-purpose office buildings. Spaces such as medical facilities, classrooms, laboratories, and workshops should be listed on the physical security design brief with the appropriate safeguards as determined by a TRA and/or threat-based design analysis. More information and examples can be found in GCPSG-015 – Application of Physical Security Zones Guide.

7. Safeguards

Safeguards for consideration may be divided into two categories: site safeguards and building safeguards. It is encouraged to use a combination of each to ensure efficacy of the safeguarding strategy. The type and number of safeguards to be used can be determined by the TRA and/or threat-based design documents and noted in the SDB for the project manager, architectural team, and other applicable parties.

7.1. Site Safeguards

Site safeguards are implemented for the site, or geographic location, of the facility. These safeguards are outside of the facility and are focused on the site itself and its features. This section is intended to be used in conjunction with guidance from GCPSG-019 – Protection, Detection, Response, and Recovery Guide, GCPSG-015 – Application of Physical Security Zones Guide, GCPSG-006 - Access Management Guide, and other listed GCPSGs when compiling an SDB for a facility.

7.1.1. Crime Prevention Through Environmental Design

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention during the designation, definition, and security design of an environment that is complementary to GCPSG-019 – Protection, Detection, Response, and Recovery Guide. Facility design and management of natural and man-made environments can enable departments and agencies to deter criminal or adversarial actions while safely managing the flow of individuals throughout a facility. These models intend to positively influence behaviour and activities while discouraging undesirable actions by staff, visitors, and potential adversaries.

7.1.1.1. Control of Site Perimeter

During public access hours, there should be no restriction on access to the site or to the Public Access Zone of the building unless otherwise determined by the TRA or Design Based Threat Analysis.

During limited-access hours, the building should be locked but with no restriction on access to the site. Signage should provide clear direction and definition of public and restricted areas of the site.

Fencing should be used for the perimeter of the site. For more information consult GCPSG-009 Security Fencing Considerations Guide. Roof access door or roof hatch should be locked with heavy-duty commercial hardware to restrict unauthorized access.

7.1.1.2. Site Illumination

Provide general illumination of building, driveways, and parking lots. For more information and recommended specifications consult GCPSG-004 Security Lighting

Considerations Guide.

7.1.1.3. Landscaping

Bushes or branches should be avoided or trimmed to maintain clear lines of sight at eye level to and from the building. Snow, grass, and shrubs should be maintained to ensure there is no visual impediment, emergency services and response personnel are not delayed, and that unauthorized access cannot be gained into or on top of the building. Loose objects such as rocks, paving bricks, benches, and tables should be secured to ensure they cannot be used as projectiles.

7.1.1.4. Site Overview

The building and the site should be observable from the roadway by first responders and passers-by unless this is deemed undesirable based on the TRA and threat-based design analysis. In multi-floor buildings, RAAs can be situated on upper floors to limit sightlines from other buildings.

7.1.1.5. Building Location

The building should not be located in an area that is susceptible to recurring natural or human-caused hazards. The building should also be in a location that is easily accessible by emergency services (fire, police, ambulance) in all conditions.

The building location should have enough space to have adequate stand-off distance as determined by a TRA.

Communication lines (telephone, data, Internet, etc.), power lines, energy supply lines (oil, gas), water, and sewage pipes should be physically protected to prevent accidental or intentional damage.

7.1.2. Easements Through Site

Easements through the site should adhere to local/provincial building regulations and/or utility company requirements (for example, Newfoundland and Labrador Hydro lists typical easement dimensions as between 3 and 15 metres). The impact of easements through a site should be considered and included in a TRA and/or Threat-Based Design.

Institutions are to be informed by the custodian of the possibility of intrusion on the site by an easement owner, such as utility crews sent to replace or repair overhead lines or excavations to repair or replace underground utilities, without advance notice to the occupants. If an easement permits public access through the site, for example in an emergency, the institution must be informed and agree with the requirement prior to occupancy.

7.1.3. Telecommunications and Data Links Outside Facility

Any physical components, including satellite equipment, should be physically protected

to prevent accidental or intentional damage. A TRA should be used to determine appropriate physical security measures for telecom wiring outside a facility. Additional information can be found in the Policy on Service and Digital.

7.1.4. Staff and Visitor Parking

Parking locations designated by signs should indicate staff and visitor parking areas. During limited access hours, staff access to indoor parking should be limited to key access or guard-controlled access.

Placement of staff parking should be considered in relation to emergency exit doors. If emergency exit doors open into the parking lot, frequent use can be anticipated, which can have impacts on reliable response.

Visitor parking should allow for easy orientation to the facility's main/visitor entrance. In order to avoid obstructions (visual or physical), there should not be space at main or side entrances for parking, stopping, or drop-off points.

7.1.5. Exterior Circulation – Roadways

Clear definition of entry points enhances legitimate access and reduces confusion. Signs should be used to direct members of the public to the proper vehicular entry points. Ensure adherence to applicable municipal and provincial/territorial requirements.

7.2. Building Safeguards

There are a variety of building safeguards that can be implemented to protect GC assets and employees, with findings from TRAs and Threat Based Design determining the which safeguard(s) may be required for a given facility and any specific requirements. Best practice is to use a combination of the following safeguards for a holistic, reliable security system (for example, utilizing Electronic Access Control and Electronic Intrusion Detection with a secure storage room to control access and detect potential unauthorized access attempts).

This section is intended to be used in conjunction with guidance from GCPSG-019 – Protection, Detection, Response, and Recovery Guide, GCPSG-015 – Application of Physical Security Zones Guide, GCPSG-006 - Access Management Guide, and other listed GCPSGs when compiling an SDB for a facility.

7.2.1. Electronic Access Control

Electronic access control safeguards provide accurate records (auditing) of visitor and employee movements throughout a facility. A TRA will determine the need for electronic access control measures and specifications of equipment. Electronic Access Control can be used in conjunction with Electronic Intrusion Detection (EID) and CCTV to ensure proper detection of attempted or actual unauthorized access.

7.2.2. Electronic Intrusion Detection Systems

Electronic Intrusion Detection (EID) systems are intended to provide continuous monitoring of vital or high value locations, access control points, zones in which access is controlled (OZ, SZ, HSZ), and any other spaces in which human supervision and control is not possible. A TRA will determine the need for electronic intrusion detection measures and specifications of equipment. EID can be used in conjunction with Electronic Access Control and CCTV to ensure proper detection of attempted or actual unauthorized access. EID must be monitored by personnel capable of coordinating a response when intrusions or emergencies occur. Best practice is for departments and agencies to establish a Security Operations Centre (SOC) to lead in this function.

7.2.3. Closed Circuit Television Systems

CCTV equipment may assist a department/agency in monitoring access to their facility, assessing valid and nuisance alarms, and providing surveillance of a problem location. A TRA and Design Based Threat analysis will determine the need for CCTV and specifications of equipment. CCTV can be combined with electronic access control and EID to ensure proper detection of attempted or actual unauthorized access, as well as initiating response. For more information consult GCPSG-011 (2024) Guide to CCTV-CCVE Systems.

7.2.4. Security Operations Centre

A SOC provides a facility to support security personnel in the monitoring, surveillance, display, control, management and response to security-related events. A SOC typically provides 24-hour surveillance activities through video camera systems, intrusion alarm sensors, and related systems. The SOC also provides the ability to detect and assess alarm notifications and dispatch staff to address the issue, such as Contracted Security teams, Commissionaires, or Emergency Services personnel. There are a number of critical functions carried out within the SOC and situational awareness is at the forefront of the operational purpose.

More information concerning the functions of using a SOC can be found at GCPSG-003 Security Operations Centre Design Considerations Guide.

7.2.5. Secure Storage Room

A Secure Storage Room (SSR) is intended to function as an approved storage container for open-shelf storage of a large amount of classified or protected information or assets. For more information on SSR construction specifications refer to G13-01 Secure Storage Room Guide.

7.2.6. Special Discussion Areas

A Special Discussion Area (SDA) is a space specially designed and managed to prevent the overhearing of discussions regarding protected and classified information at various levels of sound attenuation. For more information on SDA construction specifications

refer to GCPSG-017 Special Discussion Area Construction Guide.

8. Additional Considerations and Safeguards

GC departments and agencies operate in a considerable variety of environments within Canada and internationally. This guide cannot provide all design considerations and safeguards possible, nor does it include specific technical details for security equipment or an exhaustive list of SDB inclusions. The facility TRA and/or threat-based design will provide GC departments and agencies with most information necessary for mitigating vulnerabilities in the design of a given facility, as well as aid in decision-making on what security equipment and systems to employ.

9. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Policies, Directives, Standards and Guidelines- Canada.ca
- Canada Labour Code
- National Building Code of Canada: 2020
- National Fire Code of Canada: 2020
- International Atomic Energy Agency's Design Basis Threat
- GCPSG-003 (2021) Security Operations Centre Design Considerations Guide
- GCPSG-004 (2020) Security Lighting Considerations Guide
- GCPSG-006 (2024) Access Management Guide
- GCPSG-007 (2022) Transport, Transmittal and Storage of Protected and Classified Material
- GCPSG-009 (2022) Security Fencing Considerations Guide
- GCPSG-011 (2024) Guide to CCTV-CCVE Systems
- GCPSG-013 (2024) Fundamentals of Glazing in Physical Security
- GCPSG-015 (2023) Application of Physical Security Zones Guide
- GCPSG-016 (2022) Guide to the Facility Security Assessment and Authorization Process
- GCPSG-017 (2024) Special Discussion Area Construction Guide
- GCPSG-019 (2023) Protection, Detection, Response, and Recovery Guide
- G13-01 (07/2013) Secure Storage Room Guide

10. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-014 (2024) – Physical Security Considerations in Facility Design, for approval.

Murphy,Timothy Robert Brian,000360902

Digitally signed by Murphy,Timothy Robert Brian,000360902
Date: 2024.07.17 14:23:47 -04'00'

Tim R Murphy, CD
Manager (Acting)
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby approve, GCPSG-014 (2024) – Physical Security Considerations in Facility Design.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.07.18 13:58:24 -04'00'

Andre St-Pierre,
Director, Physical Security
Royal Canadian Mounted Police

Date