

Foundation to Hostile Vehicle Mitigation

GCPSG-025 (2026)

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

Publication Issued: 2026-10-01

Foreword

The Foundation to Hostile Vehicle Mitigation guide 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 addressing the need for a foundational guide to inform physical security functional specialist working for departments, agencies and employees of the Government of Canada (GC).

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

Reproduction

This publication may be reproduced verbatim, in its entirety, without charge, for educational and personal purposes only. Written permission from the RCMP LSA is required for use of the material in edited or excerpted form, or for any commercial purpose.

Effective Date

The effective date of GCPSG-025 (2026) – Foundation to Hostile Vehicle Mitigation is 2026-10-01

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

Foreword i
Reproduction i
Effective Date i
Record of Amendments i
1. Introduction 4
1.1. Purpose 4
1.2. Applicability 4
1.3. Equity, Diversity, and Inclusion in Physical Security Systems 4
1.4. Information Technology Considerations 4
1.4.1. Security Assessment and Authorization 5
1.4.2. Quantum Computing Considerations 5
2. Contact Information 5
3. Acronyms 6
4. Glossary 6
5. Hostile Vehicle Mitigation Function 7
5.1. Permanent Mitigation 8
5.2. Temporary Mitigation 8
6. Vehicle Dynamics Assessment (VDA) 9
7. Vehicular Threats 9
7.1. Hostile Vehicle Tactics 10
7.1.1. Vehicle-Borne Improvised Explosive Device (VBIED) 10
7.1.2. Vehicle as a Weapon (VAW) 11
7.1.3. Layered Vehicle Attack 11
7.2. Exploits 12
8. Hostile Vehicle Mitigation and Safeguards 12
8.1. Traffic Calming 12
Figure 1– Chicane Example 13
8.2. Stand-Off Distance 13
Figure 2 – Example Image of Stand-Off Distance 14
8.3. Protected Pedestrian Areas 14
8.4. Bollards and Barriers 14
Figure 3: Example Image of Installed Metal Bollards 15
Figure 4: Example Image of Installed Round Concrete Bollards 15

Figure 5: Example Image of Retractable Vehicle Security Barriers 16
Figure 6: Example Image of Deployable Temporary Vehicle Security Barriers 16
8.5. Vehicle Checkpoints 17
8.6. Temporary Closures 17
8.7. Landscaping 17
9. Standards, Testing, Product Selection 17
10. Determining Requirements 18
10.1. Threat and Risk Assessment (TRA) 19
10.2. Threat-Based Design 19
10.2.1. Threat Assessment 19
10.2.2. Information Gathering 19
10.2.3. Preliminary Analysis 20
10.2.4. Secondary Analysis 20
11. Hostile Vehicle Mitigation Project Lifecycle 21
11.1. Design 21
11.2. Build 21
11.3. Operate 21
11.4. Replace/Decommission 21
12. Crime Prevention Through Environmental Design 22
13. Reference and Source Documents 22
14. Promulgation 23

1. Introduction

The RCMP, as the Lead Security Agency 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 GC physical security functional specialists with guidance on the foundations of hostile vehicle mitigation.

1.2. Applicability

This guide applies to the development of physical security strategies for departments and agencies where vehicle-borne threats are possible. The intended audience includes physical security functional specialists, management personnel and decision makers with a risk management or risk acceptance authority within the department or agency working on the mitigation of risks posed by hostile vehicles.

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

Information technology (IT) considerations may not always be necessary when formulating plans for physical security solutions. There is however, a constantly evolving threat regarding IT systems and with the convergence of physical and IT security, the requirement to assess the risk of IT applications and software connected to a network to operate and support equipment in GC controlled buildings is critical. Examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC, etc.

1.4.1. Security Assessment and Authorization

Before implementing any applications or software that will control or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure the integrity and availability of the components, the applications, 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 IT security.

1.4.2. Quantum Computing Considerations

Departments and agencies in the GC are accountable for managing cyber security risks in their program areas, and that includes systems that operate in conjunction with physical security systems. It is important that staff across the GC are aware of the quantum computing threat and the impact it may have on the systems they use or are responsible for. Quantum computers will use quantum physics to process information and solve problems that are impractical to solve using current computing capabilities.

Cryptography, which is the study of techniques used to make plain information unreadable, and then convert it back to a readable form, is an effective way to protect the confidentiality and integrity of GC information. The future of quantum computing threatens to break much of the cryptography we currently use, and steps need to be taken to protect and "future proof" the GC. It is recommended that departments and agencies transition existing cyber security solutions to use Post Quantum Cryptography (PQC) which are algorithms that are designed to be quantum-safe but that can be run on a conventional computer. For more information on quantum computing and PQCs, department and agencies should contact the Canadian Center for Cyber Security (CCCS).

In order to properly manage the quantum threat, CCCS recommends that departments and agencies evaluate the sensitivity of their information and determine its lifespan to identify information that may be at risk. Review their IT lifecycle management plan and budget for potentially significant software and hardware updates and educate their workforce on the quantum threat. Refer to CCCS cyber security guidance ITSE.00.017 for more information.

2. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #17

Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronyms

Acronym/Abbreviation	Meaning
ASTM	American Society for Testing and Materials
CPTED	Crime Prevention Through Environmental Design
DBT	Design-Based Threat
DSM	Directive on Security Management
GC	Government of Canada
HVM	Hostile Vehicle Mitigation
IED	Improvised Explosive Device
NPSA	National Protective Security Authority (United Kingdom)
PGS	Policy on Government Security
POJ	Police of Jurisdiction
RCMP LSA	RCMP Lead Security Agency for Physical Security
SA&A	Security Assessment and Authorization
SME	Subject Matter Expert
SOP	Standard Operating Procedure
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
VADS	Vehicle Attack Delay Standard
VAW	Vehicle as a Weapon
VBIED	Vehicle-Borne Improvised Explosive Device
VDA	Vehicle Dynamics Assessment
VIP	Very Important Person

4. Glossary

Term	Definition
Asset	Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
Control of Access	Ensuring authorized access to assets within a facility or restricted areas by screening visitors and material at entry points by personnel, guards or automated means and, where required, monitoring their movement within the facility or restricted access areas by escorting them.
Design Based Threat	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.
Facility	Something that is built, installed, or established to serve a particular purpose. A facility may include a specific building (whole or part) or the site or land it is located on. The term encompasses both the physical object and its use (i.e., weapons' ranges, agriculture fields).
Hostile Vehicle Mitigation	Protective measures installed around a building or compound to prevent hostile vehicles from coming into close contact.
Insider Threat	Instances when personnel, authorized to enter or work within a GC facility, engage in deliberate actions against the GC, their employer, or their colleagues. Actions may include criminal activity, physical threats or actions, espionage, subversion, and sabotage.
Marauding Attack	Fast-moving, violent attacks where threat actors move through a location aiming to cause casualties and destroy property.
Perimeter	A continuous security line surrounding a secured zone.
Residual Risk	The risk that remains after safeguards have been selected and implemented.
Risk Tolerance	The willingness of an organization to accept or reject a given level of residual risk (exposure). Risk tolerance may differ across the organization but must be clearly understood by the individuals making risk-related decisions on a given issue.
Safeguards	Assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities.
Sally Port	A secure and controlled entry/exit featuring two sets of doors/gates, where only one opens at a time to prevent tailgating.
Stand-Off	The distance between a potential threat and the asset.
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.).

5. Hostile Vehicle Mitigation Function

Hostile Vehicle Mitigation (HVM) is a key element of physical security aimed at reducing the risks posed by vehicle-borne threats from threat actors. HVM is the selection and implementation of safeguards that are tailored to mitigate site specific threats, generally determined by conducting a Threat and Risk Assessment (TRA), then utilizing a Threat-Based

Design approach and developing safeguards appropriate for the most likely conditions of a security incident.

HVM measures are the integrated deployment of security processes, procedures, and physical barriers to counter vehicle-borne threats. They typically include a combination of physical security safeguards, security awareness and training, operational security, traffic management, and traffic calming measures.

5.1. Permanent Mitigation

Facilities and land around the facility occupied by government departments and agencies for extended periods of time, whether they are leased or owned, will likely require permanent HVM safeguards. These safeguards will be installed and maintained to provide constant protection of the facility, ensuring the day-to-day residual risk level is equal to or lower than the risk tolerance of the department or agency. Physical security functional specialists should be included as early as possible in the planning of new facilities and retrofits of existing ones to ensure physical security safeguards are included in the project plan. Permanent HVM strategies will employ a combination of mitigations and safeguards outlined in section 8 of this guide.

5.2. Temporary Mitigation

Temporary HVM safeguards are often required when there is a need to protect an area above its regular requirements. This is most commonly due to an influx of people in an area, therefore increasing the risk that it is targeted by threat actors to cause the most casualties. This may include but is not limited to:

- **Government Run Public Events:** Job fairs, public speaking events, or celebration/ceremony where members of the public will gather in mass on government property or an event space run by a government department or agency. Increased density of pedestrians will require an increase in security measures to ensure the safety of attendees and government employees.
- **Public Servant and VIP Gatherings:** When an unusually large number of public service employees gather for planned networking events, summits, or working groups, there may be a need to temporarily increase physical security safeguards at the facility hosting the event. The threat of an incident increases the larger the gathering, if VIPs are present (such as foreign diplomats, private industry elites, or high-ranking government officials), or if there is media coverage of the gathering.
- **Anti-Government Protests:** When anti-government protests are expected near or at government facilities or events, the risk of a vehicle-borne threat correspondingly increases. It is recommended that the department or agency in proximity to, or the target of, the protests work with the local law enforcement agencies that have jurisdiction (Police of Jurisdiction – POJ) to coordinate efforts to minimize risks to government assets and employees. This can include temporary road closures, deployment of temporary vehicle barriers, or minimizing staff on site for the duration of protests.

There are several factors specific to these scenarios that should be considered when conducting an assessment to determine the extent of additional temporary safeguards, including but not limited to:

- **Anticipated crowd size/density:** Events involving larger groups of people and/or densely packed crowds pose a higher risk of harm than events involving smaller groups of people and/or dispersed crowds.
- **Event duration:** As the event duration increases, the risk of harm increases.
- **Media attention/stakeholder impact:** Events that are anticipated to garner a high amount of media attention or involving marginalized groups that have been historically targeted for attack by individuals and/or groups will have a higher risk of harm than events anticipated to garner little or no media attention or not specifically involving marginalized groups.

6. Vehicle Dynamics Assessment (VDA)

A Vehicle Dynamics Assessment (VDA) is a scientific assessment of a particular site, which collects data on how various vehicle makes and models could operate, and their potential impact in an HVM event. This can provide invaluable data that can be utilized when developing an HVM strategy. The VDA methodology typically involves:

- Profiling vehicles based on size, weight, power and design;
- Analysis of potential approach routes based on existing roads, gradients, physical traffic calming measures, and surface friction to determine possible vehicle movement parameters;
- Attack vector analysis to determine potential approach angles and possible vehicle speeds;
- Assess potential vehicle movement patterns under various loads, speed, terrain and weather conditions;
- Identifying and analyzing potential vehicle escape routes for both the threat actor and evacuating civilians; and
- Evaluating existing HVM safeguards and their effectiveness in their operating environment. (Note: product test ratings are determined in controlled environments and may not perform exactly as rated in a unique operating environment).

VDAs are site-specific and may include additional considerations beyond the above examples. VDAs can be integrated into various security assessments such as a TRA, providing empirical data and vehicle specific considerations to support recommended safeguard strategies.

7. Vehicular Threats

Vehicle-related incidents have been on the rise globally due to their widespread availability and low-skill requirement to repurpose with hostile intent. Vehicle-borne threats range from

vandalism to sophisticated or aggressive attacks by threat actors, who can gain access to vehicles through several means, including but not limited to:

- Owned: a vehicle belongs to/is registered to the threat actor;
- Borrowed: a vehicle is lent by an unwitting or complicit third party;
- Leased/rented: a vehicle is hired from a company, utilizing real or fake credentials;
- Stolen: a stationary, unattended vehicle (locked or keys in ignition) is taken; and
- Hijacked: an occupied vehicle, parked inside or outside a protected area, is seized.

7.1. Hostile Vehicle Tactics

Vehicles can be utilized in a variety of ways to enable threat actors to achieve their goals. This could include using a vehicle as a weapon (VAW), such as ramming attacks against pedestrians or property. Vehicles can also facilitate the delivery or concealment of hostile devices or groups of threat actors. Regardless of the intention, hostile vehicle tactics often have indicators that can serve as an early warning that an attack is imminent. During a vehicle involved security incident, the driver is unlikely to comply with the rules of the road. Early warning indicators include, but not limited to:

- Traversing over green spaces such as fields, recreational grounds, parks;
- Parking illegally;
- Ignoring traffic signals;
- Driving at higher speeds;
- Driving on the wrong side of the road;
- Driving on sidewalks or pedestrian walking paths; and
- Entering pedestrianized zones.

7.1.1. Vehicle-Borne Improvised Explosive Device (VBIED)

A VBIED consists of an improvised explosive device (visible or concealed) located within a vehicle, which is then transported to a target. The threat actor will attempt to get as close as possible to their target to cause the maximize amount of damage. This could be a densely populated area to maximize casualties or a location critical to the target's operations, such as industrial equipment or material storage.

The threat actor may attempt to accomplish this covertly, using the vehicle to conceal the explosive device and their intent. In these cases, they will attempt to draw the least amount of suspicion, possibly using falsified documents or leveraging an insider threat to gain access to controlled areas of the target without raising alarm. A covert delivery method may be selected to allow the threat actor time to escape before the device detonates, or to have it in position to detonate later when it will have maximum effect (such as parking it near a building entrance, intending to detonate it as staff are scheduled to arrive or depart).

Alternatively, a threat actor may attempt a more direct and overt attack; the most common of which being a suicide bombing. These attacks involve the threat actor driving the VBIED directly to their target location and detonating it immediately. They may attempt a layered attack, using the delivery vehicle to transport attackers who will

dismount and continue the attack on foot before the VBIED detonates. Regardless of the goal, speed and aggression will define their approach; they will not follow traffic laws, they will attempt to circumvent or drive through obstacles and may opportunistically ram pedestrians on their approach to the target.

The effects from VBIED detonation include: the blast, fireball, primary and secondary fragmentation, and ground shock.

The blast stand-off (the distance between the device and the asset) is the most important factor in determining the extent of damage that can be caused. Maximizing the blast stand-off distance will reduce the damage sustained to the asset. The effects and mitigation of an explosive device attack is covered in more detail in GCPSG-002 Blast Mitigation Considerations Guide.

7.1.2. Vehicle as a Weapon (VAW)

Vehicles themselves can be the primary tool in a threat actor's plan, utilizing its mass and speed to attack a target. Sometimes called a ramming attack; using a vehicle as a weapon is the intentional act of driving a vehicle:

- At an individual or into crowds of people to cause casualties; or
- Deliberately driving a vehicle into infrastructure to damage or disrupt its operation. This may indirectly lead to harm to people, disruption to the operation of a site/event, or more widely, critical services or supplies.

Driving a vehicle into crowds is regarded by threat actors as attractive because it is likely to cause multiple casualties, is low complexity, affordable, requires little planning and skill, and is perceived as less likely to be detected in the planning phase. Roads that have extended straight sections clear of obstructions and a lack of physical delineation between vehicle areas and pedestrian areas (such as bollards) increase the vulnerability of a location to a VAW attack.

VAW attacks are frequently the first part of a Layered Attack. These attacks often begin on public roads with little or no warning and may be followed by a marauding attack using bladed weapons, firearms, or hand-thrown hostile devices.

7.1.3. Layered Vehicle Attack

A layered vehicle attack, also known as a complex vehicle attack, is a combination of attack types. Layered attacks are much more sophisticated, requiring more planning and resources and they are extremely devastating if carried out successfully.

In a layered vehicle attack, a threat actor will employ a combination of two or more of the following tactics:

- Facilitating the delivery of armed attackers, either covertly or overtly;
- Delivering or concealing a VBIED;
- Conducting a VAW attack, either as a diversion or a primary effort; and
- Executing a secondary attack targeting first responders or evacuation points.

7.2. Exploits

There are seven exploits that threat actors may use to overcome operational or physical security measures. Each of these exploits should be considered when analyzing vulnerabilities as part of risk management activities and threat assessments. The seven exploits are:

- **Parked:** A vehicle may be legally or illegally parked close to, or inside the perimeter of a facility. Prior to an attack, a vehicle may repeatedly park in the same area to create familiarity and may be abandoned for a short or considerable time;
- **Encroachment:** A vehicle may exploit gaps in perimeter protection, drive slowly through, or over, what is perceived to be a perimeter, or tailgate legitimate vehicle access through a single-layer vehicle checkpoint;
- **Penetrative:** A vehicle may be used at low or high speed to breach security measures. Lower speed attacks may involve the vehicle being used aggressively and repetitively rammed against security measures or other obstructions to gain access;
- **Deception:** Attackers may forge or steal documentation, lie, or alter the look of their vehicle or themselves to appear legitimate. A 'Trojan Vehicle' is a vehicle modified to replicate a legitimate access. An 'unknowing mule' is a legitimate driver who unknowingly delivers an IED, weapons, and/or attackers into a site;
- **Coercion:** A legitimate driver, security staff at a vehicle checkpoint, or employees could be forced to facilitate access to a site. They, or others known to them, may be threatened with violence or placed under undue influence through mental pressure such as bribery or blackmail;
- **Insider Threat:** A person with legitimate access willingly facilitates or enables an attack by operating the security measures locally or remotely, managing or issuing access rights, or interfering with security measures; and
- **Sabotage:** A cyber or physical attack aiming to alter, weaken, or disable a barrier, while intending to leave no evidence.

8. Hostile Vehicle Mitigation and Safeguards

When implementing hostile vehicle mitigations and safeguards, a wide range of potential tactics can be used, each offering its own set of advantages. Selecting the most appropriate strategy requires careful evaluation of the specific context, weighing factors such as the nature of the threat, the environment in which the measures will be deployed, and the balance between security, accessibility, and operational convenience. By thoroughly assessing the strengths and weaknesses of each option, security functional specialists can ensure that the chosen safeguards are both effective and proportionate to the risks at hand.

8.1. Traffic Calming

Traffic calming involves the use of design features and physical measures to reduce vehicle speeds and control traffic flow in the areas identified that need HVM and safeguards. Examples of how this is achieved include speed bumps, chicanes, narrowed lanes, raised crosswalks, and textured road surfaces. By slowing down the flow of traffic, these measures

can help reduce the likelihood and severity of hostile vehicle attacks while also improving pedestrian safety.

Figure 1– Chicane Example



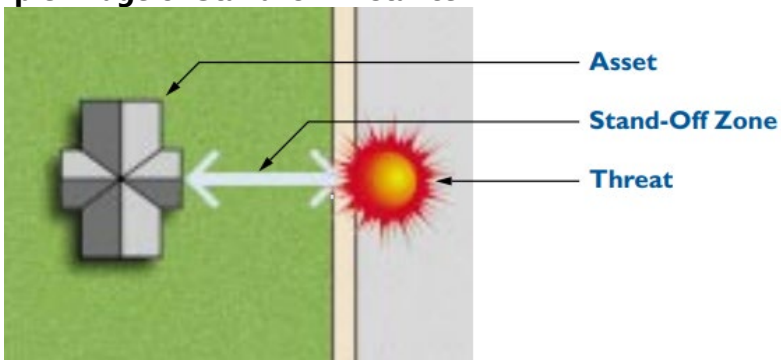
Source: Aerial View Famous Lombard Street San Stock Photo 1538941079 | Shutterstock

Alt text: Figure one depicts an aerial view of Lombard Street, San Francisco, as an example of chicanes.

8.2. Stand-Off Distance

Stand-off distance is the intentional space maintained between a potential vehicular threat and the protected asset, building or crowd. The buffer zone created reduces the impact force of a VBIED and provides security personnel with more time to detect, assess and respond to threats. Stand-off distances can be achieved through landscaping, controlled access points, or the strategic placement of barriers. A more in-depth review of explosive mitigation, including stand-off distance, can be found in GCPSG-002 Blast Mitigation Considerations Guide.

Figure 2 – Example Image of Stand-Off Distance



Source: U.S. Airforce Installation Force Protection Guide

Alt Text: Figure two depicts an example image of stand-off distance, showing the asset and the threat separated by arrows depicting stand-off distance.

8.3. Protected Pedestrian Areas

A protected pedestrian area is an area that is designated for and accessible to foot traffic exclusively. A pedestrian protected area must have a physical perimeter fully encompassing the space, with barriers rated to an appropriate level to stop vehicle collisions from penetrating into the protected area. Any vehicle access points into a pedestrian protected area, either for emergency response or maintenance, should be access controlled and immediately secured after approved vehicles pass through. Retractable bollards or crash rated gates may be considered for access points. Areas to consider developing as pedestrian protected areas include public transit waiting areas, footpaths, areas adjacent to building entrances and exits, and areas where vehicle traffic and pedestrian movement coexist near each other.

8.4. Bollards and Barriers

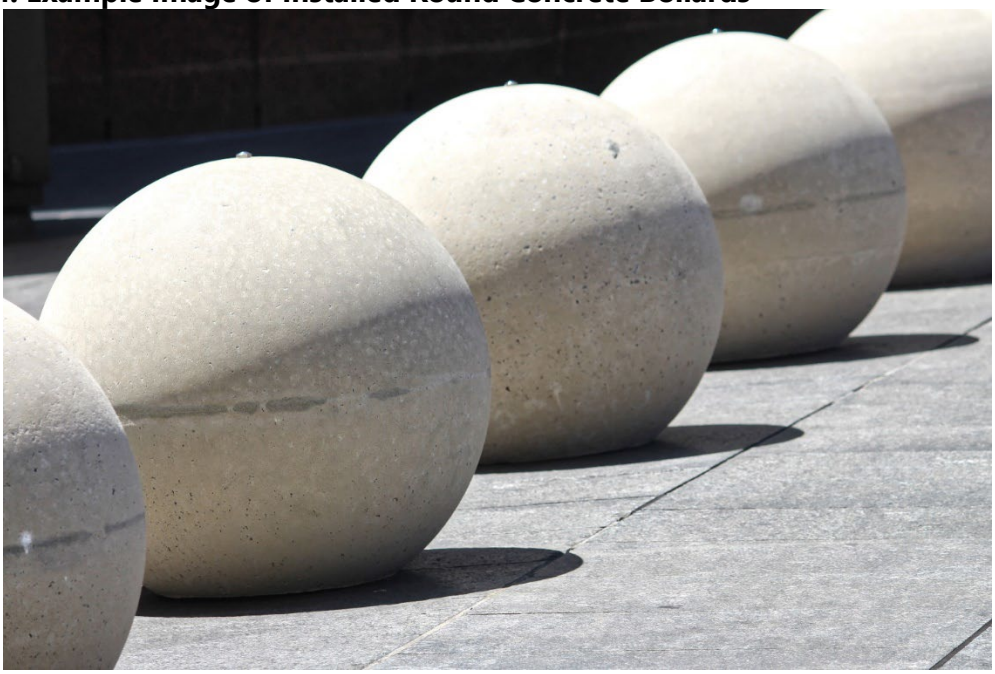
Bollards and barriers are fixed or removable physical security structures designed to prevent unauthorized vehicle access to protected zones. They can be made from steel, reinforced concrete, or other high-strength materials, and may be permanent, retractable, or temporary. In addition to their security function, bollards can be integrated into the site's aesthetic design, blending in with street furniture to maintain an inviting design.

Figure 3: Example Image of Installed Metal Bollards



Source: Stainless Steel Bollard Entering Pedestrian Area Stock Photo 1409046014 | Shutterstock
Alt text: Figure three depicts a row of installed metal bollards.

Figure 4: Example Image of Installed Round Concrete Bollards



Source: Row Round Concrete Bollards Shape Sphere Stock Photo 1929188162 | Shutterstock
Alt text: Figure four depicts a row of installed spherical concrete bollards.

Figure 5: Example Image of Retractable Vehicle Security Barriers



Source: Automatic Bollards Retractable Lifting Bollards Enable Stock Photo 1715463778 | Shutterstock

Alt text: Figure five depicts metal retractable vehicle barriers in the extended position.

Figure 6: Example Image of Deployable Temporary Vehicle Security Barriers



Source: Red Retractable Security Barrier Install Pedestrian Stock Photo 2717133665 | Shutterstock

Alt text: Figure six depicts a deployed ARMIS ONE mobile vehicle barrier.

8.5. Vehicle Checkpoints

Vehicle checkpoints are controlled entry points where vehicles are stopped, inspected, and verified before being allowed access to a secure area. These checkpoints may include security personnel, vehicle scanning technology, and barriers that can be raised or lowered as needed. Vehicle checkpoints can be designed as a sally port to provide additional security and prevent tailgating. A sally port is a secure entrance design featuring two gates that do not open at the same time, a vehicle would pass through the first gate and wait for it to close behind them before the second opens to permit access to the facility. To function properly, the space between the two gates must be isolated by vehicle barriers to ensure a vehicle must pass through both gates in turn to enter the facility. Vehicle checkpoints can serve as both a deterrent and a detection measure, ensuring that only authorized vehicles are allowed access to designated areas. Vehicle checkpoints can be permanently installed or temporarily set up as needed.

8.6. Temporary Closures

Temporary closures involve restricting vehicle access to certain streets or areas for a defined period of time, often during high-profile events, elevated threat levels, or emergency situations. Closures can be enforced using temporary barriers, security staff, or police presence, and are particularly effective for managing short-term risks without requiring permanent infrastructure modifications. This will require coordination and permission from the local authorities or POJ who manage the roadways.

8.7. Landscaping

Landscaping can be used in various ways in an HVM strategy, either as a complimentary layer or an element of another safeguard's application. Traffic calming measures are commonly enabled by purpose designed landscaping. There is some intersectionality between security barriers and landscaping, such as planters being tested and rated using the same standards used by bollards and barriers. Dense forests or particularly large trees may be considered when developing an HVM strategy, achieving a similar mitigating effect as barriers and bollards. If included as part of an HVM strategy, forests and trees should be assessed by an engineer to ensure they provide the necessary level of protection. Any trees or forest used as part of an HVM strategy should be on the facilities property, and removal of the trees or forests should only be considered if replacement safeguards are implemented in advance. Berms and ditches may also be implemented to increase the effectiveness of other safeguards, such as installing a ditch before a crash rated fence. Any landscaping that is being utilized as part of an HVM strategy should be reviewed and approved by qualified engineers to ensure the planned landscaping will have the desired effect against a hostile vehicle.

9. Standards, Testing, Product Selection

It is recommended that a barrier deployed to mitigate the risk to assets posed by vehicle-borne threats be a 'Rated Vehicle Security Barrier' that has undergone formal vehicle-impact testing. The testing standards are not interchangeable; if a TRA has identified a specific standard level it

should not be deviated from unless additional analysis confirms alternative standard levels would be appropriate to mitigate the risk to an acceptable level. Listed below are recognized vehicle impact standards that are used to measure the effectiveness of an HVM measure:

- International Organization for Standardization ISO 22343-1:2023 Security and resilience — Vehicle security barriers Part 1: Performance requirement, vehicle impact test method and performance rating
- American Society for Testing and Materials (ASTM) F 2656 – Standard Test Method for Crash Testing of Vehicle Security Barriers; and
- NPSA Vehicle Attack Delay Standard (VADS). VADS provides a means for testing Vehicle Security Barriers against aggressive and repetitive vehicle impacts. HVM Standards blog.

While test methods vary slightly across standards, they all assess how an HVM measure performs under a specified impact. This given impact is often determined by impact vehicle type (such as passenger vehicle vs. heavy vehicle), the weight of the impact vehicle, speed of the impact vehicle, impact angle, and penetration distance (such as the distance between the impact point and the point where the vehicle is immobilized).

10. Determining Requirements

When developing safeguard requirements for an HVM strategy, particular attention should be paid to considerations determined by both the site and assets being protected, and the potential types of hostile vehicles that may manifest as threats. Things to consider are:

- Maximum potential speeds (such as length of roads with a straight shot to the asset);
- Size of vehicle (such as commercially available or personal); and
- Types of attacks (such as VAW, VBIED, or layered).

There are several methodologies to assist in determining HVM safeguards requirements. A TRA is the most holistic approach, as it considers the widest range of data points to assist with determining appropriate and proportional requirements. Requirements can also be determined by utilizing DBTs, which require less resource investment than a TRA, but in turn contains less evidence to support the decision. Once the nature of threat is understood, functional specialists should take a methodical approach to determine project requirements and identify vulnerabilities. The following factors are identified as being useful in assessing risk at each access point:

- **Straight length distance into the site:** Lengthy straight approaches into facilities and event grounds give hostile drivers an approach that allows them to accelerate to higher speeds, increasing the likelihood of penetrating barriers. Locations with long straight approaches pose a higher risk of harm than locations with short or curvilinear sections.
- **Roadway width:** The width of the roadway affects the speed of vehicles. It is easier to reach higher speeds on a roadway with a wide cross-section (such as a six-lane arterial road) compared to a roadway with narrow lanes and on-street parking along curb lanes.
- **Posted speed limit:** As the posted speed limit of a roadway is often designed based on roadway characteristics such as width, presence of a physical median, surface type,

roadside objects, and presence of pedestrians. The posted speed limit of a roadway is a good indicator of the minimum speeds a hostile driver can achieve on the roadway. Roads with higher posted speed limits will likely permit hostile drivers to travel at higher approach speeds to an entry.

- **Distance to signalized intersection:** Hostile drivers forced to stop at a signalized intersection provide natural barriers that could prevent them from accelerating to higher speeds when approaching an access point.
- **Stand-off distance:** Stand-off distance is the distance available between the HVM measures (such as barriers, gates) and the target. The available stand-off distance will determine the type of measure that needs to be used and the location of the installation.

10.1. Threat and Risk Assessment (TRA)

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.

10.2. 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 discussed in GCPSG-014 Physical Security Considerations in Facility Design. 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 TRAs should be used in tandem. The steps in threat-based design are:

10.2.1. 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.

10.2.2. 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.

10.2.3. 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; and
- Attractiveness of Target.

The outcome of this phase is a threat assessment document outlining the threat environment and all known threats and vulnerabilities that must be considered. TRA information may be used in the development of the threat-based design document.

10.2.4. 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 capability to harm. Threats with higher relevance should be considered more likely when compared to those with less relevance. Threats with similar attributes can be grouped into defined threat types based on shared characteristics. Within these broader threat types, additional considerations may include site and activity specific factors such as operational procedures, the facility's location and accessibility, and the transportation modes or routes to and from the site. The information analyzed is then compiled into a document outlining an overview of the threat, as well as its attributes, characteristics and likelihood relating to the facility. The results of this document as well as the TRA can be used to develop the HVM strategy for the facility.

11. Hostile Vehicle Mitigation Project Lifecycle

Every safeguard should have a lifecycle management plan that covers everything from procurement to decommissioning or replacement.

11.1. Design

An HVM strategy needs to be developed before it is installed. Implementing the physical security requirements into a project at the earliest stages can reduce costs and ensure Standard Operating Procedures (SOPs) are developed in conjunction with the added HVM safeguards. It is important to include data collected in initial TRAs at this point in the project to ensure the HVM strategy is addressing the specific threats faced by the facility.

Understanding the capabilities and limitations of individual products and strategies is vital before they are procured. This includes ensuring they are installed correctly to maximize the vehicle resistance and ensure products perform to the level for which they are certified.

11.2. Build

Once an HVM strategy has been completed, it is important to ensure it is built as per instruction, as this will maximize the vehicle resistance. A poorly or improperly built safeguard may create vulnerabilities that prevent the safeguard from functioning as expected. Due care and attention must be given during installations to ensure products are installed as per manufacturer's instructions. It is recommended that physical security functional specialists and subject matter experts (SME), familiar with the build requirements, periodically assess the installation process to ensure compliance with the installation requirements, as well as applicable municipal, provincial, territorial, and federal standards and requirements.

11.3. Operate

When the HVM safeguards are installed, it is important to keep them well maintained. Inadequately maintained equipment will inevitably fail or lead to degradation, increasing the likelihood of an incident or resulting in higher costs due to replacement. This could also have an impact on the security operations of the facility, creating vulnerabilities that can be exploited by a hostile vehicle.

11.4. Replace/Decommission

A plan should be in place for the replacement and/or decommissioning of each safeguard. This can include factors such as how long physical equipment is expected to last before requiring replacement. Conditions to consider include frequency of use, weather conditions, and frequency of preventive maintenance. Any associated contracts should be considered as well, such as maintenance contracts or hired private security operating equipment.

12. 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.

13. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service
- Directive on the Duty to Accommodate
- Guide for Two-Spirit, Transgender, Non-Binary, and Gender-Diverse Employees
- Ontario Traffic Council Hostile Vehicle Mitigation Measures (January 2023)
- U.S. Airforce Installation Force Protection Guide
- GCPSG-002 Blast Mitigation Considerations Guide
- GCPSG-019 – Protection, Detection, Response, and Recovery Guide
- GCPSG-014 Physical Security Considerations in Facility Design
- Design Basis Threat (DBT) | IAEA
- GCPSG-022 (2024) Threat and Risk Assessment Guide
- HVM - Impact Rated | NPSA

14. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-025 (2026) – Foundation to Hostile Vehicle Mitigation, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2026.10.01 12:57:55 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby recommend, GCPSG-025 (2026) – Foundation to Hostile Vehicle Mitigation, for approval.

Bissonnette,Philippe Yvon,000133440

Bissonnette,Philippe Yvon,000133440
2026.10.02 11:01:37 -04'00'

Philippe Bissonnette,
A/Director, Physical Security
Royal Canadian Mounted Police

Date