Fundamentals of Detection Systems in Physical Security

GCPSG-021 (2025)

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

Publication Issued: 2025-04-25
Updated: YYYY-MM-DD

Royal Canadian Mounted Police Gendarmerie royale du Canada

Canada

Foreword

Fundamentals of Detection Systems in Physical Security 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 implications detection system selection has on physical security 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-021 (2025) – Fundamentals of Detection Systems in Physical Security is 2025-04-25

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 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 guide is to inform departments and agencies of a variety of available detection systems for use in a departmental physical security management program. Included in this guide are the application and efficiency of these detection systems as safeguards to minimize risks to the people, information, and assets of the GC.

1.2. Applicability

This guide applies to GC security functional specialists assigned physical security responsibilities in the protection, detection, response, and recovery functions of any GC facility or property. This also includes property management personnel and decision makers with a risk management or risk acceptance authority within the department or agency.

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

All employees of the 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 GC 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 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/Abbreviation	Meaning
CCTV	Closed Circuit Television
CDE	Chemical Detection Equipment
CPTED	Crime Prevention Through Environmental Design
EDI	Equity, Diversity, and Inclusion
EID	Electronic Intrusion Device
GC	Government of Canada
HSZ	High Security Zone
OZ	Operations Zone
PDRR	Protection, Detection, Response, Recover
PVC	Polyvinyl Chloride
RCMP LSA	RCMP Lead Security Agency for Physical Security
RZ	Reception Zone
SA&A	Security Assessment and Authorization
SOC	Security Operations Center
SOP	Standard Operating Procedures
SZ	Security Zone
TRA	Threat and Risk Assessment

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.
Chemical Warfare Agents	Extremely toxic synthetic chemicals that can be dispersed as a gas, liquid or aerosol or as agents adsorbed to particles to become a powder, that have either lethal or incapacitating effects on humans.
Compartmentalization	A non-hierarchical grouping of assets used to control access more finely than with hierarchical security classification alone.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.
Cutting Agents	Adulterants that are added to illicit drugs in order to modify their physiological properties, and/or inert substances that are added solely to increase product bulk.
Defense-in-depth	This is the principle where security zones are implemented in a progressively restrictive manner, proceeding from the least restrictive zone to the most restrictive.
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)
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.
Mitigation	Activities taken to reduce risks.
Narcotics	A drug or other substance that affects mood or behavior and is consumed for nonmedical purposes, especially one sold illegally.
Need-to-access	The principle that there is a need for the person to access the area or zone in order to perform their duties. This is not to be confused with the need-to-know the content of the information contained or processed within that area or zone.
Need-to-know	The principle that there is a need for someone to access and know information in order to perform their duties.

Precursor Chemicals	Precursor chemicals are chemicals that are essential to the production of a controlled substance. Precursor chemicals have a wide legitimate use in the production of consumer goods such as pharmaceuticals, fragrances, flavouring agents, petroleum products, fertilizers and paints. For example, ephedrine and pseudoephedrine, commonly used in cold and decongestant medicine, are precursor chemicals that are used to produce methamphetamine.
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.
Vulnerability	An inadequacy related to security that could increase susceptibility to compromise or injury.

5. Detection Systems

Detection systems are mechanical, electrical, or procedural systems designed to alert security of specific conditions being met which may indicate the presence of an item or situation requiring a response. A detection system can be as simple as a tripwire attached to a bell on one end of the spectrum, with complex multilayered infrared camera systems on the other end. Regardless of the complexity of the system they are all designed to achieve the same purpose; the detection of people, objects, chemicals, or other such interlopers. Various common detection systems are explored throughout this guide, as well as best practices related to their selections and operation, and how they can fit into a larger security portfolio.

6. Alarm Systems

An alarm system consists of multiple safeguards all linked to create a mitigation effort that is more than the sum of its parts. When designing an alarm system, each component of Protection, Detection, Response, and Recovery (PDRR) should be considered and if possible, a part of the alarm system should address each element. A complete alarm system should be able to generate a response to any activated alarms by deploying security or law enforcement personnel. It is also best practice to have CCTV connected to the alarm system, so security personnel can view what is happening in an area when an alarm is triggered or pull footage to be used as evidence. CCTV systems can be programed to begin recording an area anytime a detection device is triggered, as well as signaling to the operators that a specific area requires observation to determine if a sensor detected a real or perceived threat. Alarm systems should be connected to backup power when applicable, and wireless connections should be avoided to minimize the risk of interception, disruption, or unauthorized remote access.

There are two ways to monitor an alarm system, onsite or offsite monitoring. Onsite monitoring is often the preferred method when practical, as a response can be generated immediately by the onsite security team. Onsite monitoring also minimizes the risk of a loss of communication between the alarm system and the operators, as they can be hardwired in a closed system. Offsite monitoring has its advantages as well, often saving costs over having dedicated on site security. Offsite monitoring can be sufficient for less valuable assets, but is generally inadvisable for the protection of highly sensitive or valuable assets. Offsite monitoring services are often provided by third parties and it is incredibly difficult to get accurate data on the efficiency of their response times, as monitoring services will often employ sub-contractors to check the site after an alarm is triggered. These multiple layers of external contractors can complicate the process of screening any potential responders and open up multiple vulnerabilities that are incredibly difficult to mitigate. Due to this, offsite or third-party monitoring should be considered only when other options prove infeasible.

6.1. Electronic Intrusion Devices

Electronic intrusion devices (EID) are automatic detection systems that often make up a component of a facility's security profile. EID systems operate by monitoring various conditions in their area of operation and notify when conditions change in such a way that may indicate the presence of a person. EID systems do not typically generate a response on their own, requiring supplementary systems to investigate the cause of the alarm. This is often done utilizing CCTV and security patrols to follow up on EID systems being triggered. EID is a resource effective way to monitor large facilities where it may not be practical to have security staff constantly monitoring the entire site; instead deploying resources only to areas with unverified activity requiring investigation. Another benefit of EID is detecting unscheduled access to a site and notifying security personnel or law enforcement, such as detecting movement in an office when it is expected to be unoccupied. In any case, EID systems provide a detection element only and will require additional safeguards to provide the response and recovery elements to ensure threats are properly mitigated.

6.1.1. Vibration Detectors

Vibration detectors are most commonly installed on fences, however specialized versions exist which can detect ground, vault, window and safe vibrations as well. Vibration detectors trigger an alarm when a set level of vibration is detected. These levels are often custom set to specific parameters to limit the amount of false alarms. A vibration detector on a fence will often be calibrated to trigger an alarm when a human attempts to scale the fence, but not when smaller animals or weather conditions may cause smaller levels of vibration.

6.1.2. Motion Detectors

A motion detector is a device that can sense motion in a fixed area that has line of sight to the detector. Motion detectors can often be calibrated to trigger an alarm based on the amount of motion sensed. This can limit false alarms by only triggering alarms for movements that are approximately the size of a human. Cheaper models may not have a feature like this, making them more prone to false alarms caused by non-nefarious movement (such as posters moving near a vent and/or rodents).

6.1.3. Tomographic Sensors

Tomographic sensors are a type of motion sensor that utilizes disruptions in radio waves to identify movement. Unlike traditional motion sensors that require line of sight, tomographic sensors can be placed out of sight and are able to function through walls and furniture. This is done by setting up multiple sensors surrounding the area that is being monitored. The tomographic sensors monitor the radio waves between them, and will trigger when these radio waves are disrupted, indicating something has moved through the area. Tomographic sensors are sensitive enough to detect an animal the size of a small dog however will not be triggered by movement anything smaller than that. This minimizes false alarms caused by small rodents, insects, or air currents from a vent or window affecting curtains or other fabric.

6.1.4. Glass Break Sensors

Glass break sensors are designed to detect the sound of breaking glass. As they sense audio, a single glass break sensor can cover a room with multiple windows. A noisy environment however usually diminishes the detection capabilities of the device. Glass break sensors can add an additional layer of detection and works well as part of a larger security system but their abilities are limited when used independently.

6.1.5. Contact Sensor Alarms

Contact sensor alarms consist of two sensors that can determine when they are in touching, or are within several millimeters of each other and alert a system when the contact is broken. They are most commonly employed on doors and windows, with one sensor being installed on the frame, and the second installed on the door or window. They must be installed so that they are in contact with each other when the desired state of the equipment is met, usually when the door or window is closed. An alert is sent to the monitoring system whenever the contact is broken between the two sensors, such as when a door or window opens during quiet hours when no activity is expected. Contact sensors can also provide information to a security team, letting them know when doors are opened on site without triggering an audible alarm.

It is possible to integrate contact alarms to larger security systems as an additional layer of detection. An access control system could be linked to contact alarms and programmed to limit false alarms. This can be achieved by programming the alarm to only trigger if a valid access card is not scanned before the door opens, or designating hours when the alarm is always active such as when the office is closed and no permitted activity is anticipated.

6.1.6. Photoelectric Sensors

Photoelectric sensors are emitters and receivers that create a beam of light between them and will trigger an alarm if the beam is disrupted. This creates a virtual tripwire, capable of alerting a response element without the person being aware that they have been detected. Alternatively, they can be set up to monitor a specific physical asset by placing the asset directly between the emitter and receiver, triggering an alarm when the asset is removed and the beam connects the emitter and receiver. Photoelectric sensors can be installed quickly for relatively low cost and are especially effective in providing compartmentalized detection in an area where motion detectors may be ineffective due to a high volume of permitted movement. Museums are a good example of where a photoelectric sensor would be more effective than a motion detection system; they can alert security personnel when a person gets too close to an exhibit, but would not cause false alarms due to others moving around the room.

7. Visual Monitoring

Visual monitoring is the most basic form of detection and comes with its own benefits and vulnerabilities compared to more complex systems. Visual monitoring can be as basic as simple observation by security staff or aided by electronic surveillance systems such as CCTV linked to a monitoring station. A benefit to visual monitoring is the ability to immediately triage incidents that equipment may not have the capacity to properly analyze. Detection systems trigger alarms based on specified changes in the environment, they cannot determine what is happening beyond that and require investigation to determine what tripped the alarm and if it is nefarious or benign. Visual monitoring allows for immediate decisions to be made by security staff; seeing a person attempting to scale a fence provides more immediate information than a vibration detector being triggered. A notable shortcoming of visual monitoring is the human element; a guard or CCTV operator is only as effective as their attentiveness and training allows. Poorly trained or inadequately staffed security teams may not have the capacity to effectively monitor an area with visual detection alone; they are most effective when combined with EID to assist in directing their attention to areas with unverified activity.

7.1. CCTV Assisted Monitoring

CCTV systems are connected networks of equipment designed to capture, transmit, display, and store imagery data. CCTV systems range in complexity from a single camera connected to a display monitor, up to networked systems capable of monitoring and controlling hundreds of cameras connected locally, remotely, and globally.

These systems can be accompanied by software that can identify and alert to changes to what the system is observing, providing a similar function to motion detection. These programs operate by triggering an alert when a specified visual change is observed by the monitoring software, generally caused by movement in the area being observed. The software detects visual changes and not true movement, so these programs are subject to false alarms caused by changes in lighting conditions or other non-movement related changes to the visuals. This can be partially mitigated by calibrating the amount of change needed to trigger an alert, and identifying specific sectors of the monitored area to detect visual changes, such as entry points and travel routes. This software is most commonly used to initiate recording when there is perceived activity, saving storage space and extending the length of time recordings are retained before overwriting occurs. Any notable disruption in one or all cameras within a system should be immediately and thoroughly investigated.

More information on CCTV systems and their applications can be found in GCPSG-011 Guide to CCTV-CCVE Systems.

7.2. Personnel Based Monitoring

Personnel can be relied on in a limited capacity to detect incidents in either a dedicated or passive model. A dedicated model is the most commonly utilized, and includes security personnel conducting patrols, CCTV operators, sentries/access control guards, and properly trained reception employees. One of the primary responsibilities of these staff is to be on the lookout for persons attempting to enter the facility, and they should be trained on how to respond to, or alert, security staff should an unauthorized or suspicious person be observed. In addition to monitoring the movements of individuals, personnel can be utilized to identify objects carried or planted and communicate that information to security staff as required. As an example, an individual carrying an umbrella compared with an individual carrying a baseball bat would require vastly different approaches from security staff. This is a distinction that detection equipment alone may not be able to reliably make.

Passive models of personnel based monitoring is the byproduct of a risk aware and security trained workforce. This incorporates staff whose primary duties do not involve monitoring areas, but have received the training to identify and report suspicious or unusual incidents to security staff for investigation. Passive models of monitoring should not be relied on as a dedicated safeguard, but as a supplementary layer of protection to enhance the dedicated detection systems in place. Passive detection alone is often unreliable as it is proportional to staff's security awareness and training, willingness to report suspicious activity, and likelihood of noticing unauthorized persons in restricted access areas. This type of detection is most effective in smaller facilities, where staff know and recognize each other and will notice anything unfamiliar in their facility.

7.3. Training and Implementation

When visual monitoring is a planned element of a facility's detection system, there should be an emphasis on training, and maintenance of these skills especially by employees conducting patrols and monitoring surveillance equipment. Visual monitoring is directly proportional to the aptitude and attentiveness of the security team. Even the most comprehensive surveillance system is entirely ineffective if the person monitoring it is not paying attention to it or is not trained on how to handle observed incidents. When determining the potential of visual monitoring to detect threats, only employees dedicated to the task should be included in any risk mitigation calculations. Passive monitoring by staff who are security trained and aware is not as reliable or measurable as staff trained and employed specifically for the detection of individuals both permitted and trespassing. There are several categories of visual monitoring to consider, explored in Table 1: Visual Monitoring and Training Recommendations.

Table 1: Visual Monitoring Training Recommendations

Personnel Category	Recommendations
CCTV/SOC Operators	• Operators are trained on the site's equipment; • Operators know who to call for maintenance of equipment; • SOP has been developed for who to contact (onsite security or local law enforcement) in the event of an incident; and • Operators are trained on how to prepare and authorize the release of footage for investigations.
Patrolling Guards	• SOPs are available to ensure that guards have information on what actions to take during different events/incidents; • Guards are trained and familiar with privileges associated with certain access badges; • Guards are trained and certified in use of force when intervening; • Guards understand the area(s) over which they have authority; • Guards are trained on who to contact should assistance be required (emergency services, backup guards, and/or site supervisor); and • Guards are trained on reporting and escalating incidents.
Sentries/Access Control Guards	• SOPs are available to ensure that guards have information on what actions to take during different events/incidents; • Guards are trained on access control requirements; • Guards are trained in effective tracking of persons on site; • Guards are trained and certified to use the appropriate level of force to prevent forceful unauthorized entry attempts; and • Guards are trained on who to contact should assistance be required (emergency services, backup guards, and/or site supervisor).
Reception Staff	• Staff are provided security awareness training to empower them to spot and deal with suspicious behavior; • Staff are trained on who to contact for assistance, or to escalate a suspicious event (site security or local emergency services); • Staff are trained on how to safely handle an incident while awaiting a response from security or law enforcement; and, • Staff are trained on how to safely disengage from an incident and find a safe/secure location to await assistance when necessary.
Security Aware Staff	• Staff are provided security awareness training to empower them to spot and deal with suspicious behavior; • Staff are trained on when and how to challenge an individual not displaying the proper badge for a zone; • Staff are trained on how to report suspicious incidents to site security for investigation or intervention; and • Staff are provided safety training on when to disengage or remove themselves from a situation to allow security personnel to handle it.

8. Contraband Detection

A key part of security is ensuring positive control on what can and cannot be brought into/out of a facility or carried by an individual. The detection of prohibited items at the point of entry can help ensure the safety of personnel and visitors, as well as limit the ability for hostile threat actors to introduce items that may be used to circumvent subsequent layers of defense. Some commonly banned items include; weapons, tools, video and audio equipment, intoxicating substances, and unidentified liquids and powders. Although not necessarily illegal, common items may pose risks if allowed into a secure facility. It is not illegal to carry tools in a backpack, however, allowing visitors to bring them into a facility greatly increases the risk of them being used to disable or circumvent mitigation efforts or injure staff. Prohibited items should be clearly identified by signage and reinforced by security personnel at the point of entry. A TRA should be conducted to determine what items (if any) should be banned from entering a facility.

8.1. Metal Detection

Metal detectors are commonly used to detect and mitigate the risk of prohibited items being introduced to a controlled area. They are often used in areas that are open to the public however are at risk of being targeted by threat actors. These are commonly used at sporting events, cultural & historic sites, transportation hubs, education campuses and government buildings. Metal detectors are a component of a manned checkpoint, and will have one or more security guards operating the equipment. Metal detectors come in two common types, often deployed together for greater efficiency. These are the "walk through metal detector" and the "hand-held wand". At checkpoints with metal detectors people walk through first, and anyone who alerts at the walk-through detector are searched with a hand-held wand to pinpoint the metal object and determine if it is permitted or prohibited.

8.1.1. Walkthrough

A walkthrough detector has a person walk through a detector the size of a doorway, which will trigger an alarm if enough metal is detected. They are commonly calibrated to detect items as small as a folding knife. Some more advanced models can identify what area within the detection zone triggered the alarm and alerts the operator to roughly where on the person the metal was detected. For example, if the lower part of the detector activates, it may indicate items are hidden in a boot or sock.

8.1.2. Handheld

Security wands are handheld devices that can pinpoint an area with metal with greater accuracy than a walk-through sensor. They can be used independently or as a secondary check once the person triggers a walkthrough detector. When used, a security guard would have a person stand still with their arms out and their legs separated. The security guard would then move the wand along both sides of each limb, and on the front, back and sides of the body. The wand will trigger when metal is detected directly under it. This is much more precise than a walk-through detector but it is time consuming.

8.2. X-Ray

Similar to metal detectors, the primary function of X-Ray machines is to detect unauthorized items before they are introduced to a controlled environment. These machines commonly scan bags and equipment however, some models are designed to screen people. X-Ray machines require trained security personnel to operate them. Security personnel will also conduct secondary searches as necessary, and seize any items they have the authority to confiscate. X-Ray machines reveal the contents of a container, or items hidden on a person and some devices are capable of identifying threats autonomously. A well-trained operator will be able to accurately identify metal objects, wires and electronic components, liquids, and plastics, and determine whether the person or container requires a secondary physical inspection. An X-Ray machine is able to mitigate the risk of nonmetallic threats by allowing operators to see the shape and material of concealed items, and can be effective at detecting hostile devices that may not contain enough metal to be identified by a metal detector (such as plastic printed firearms, ceramic blades, plastic explosives/PVC pipe bombs, or noxious chemicals in nonmetallic containers).

X-ray machines will often be deployed alongside metal detectors where there is a reasonable expectation that guests or employees will be carrying bags, such as transportation hubs, courthouses, and historic sites open to the public. An X-ray machine is less invasive and time consuming than physically searching every bag, and can identify items sewn into the lining of bags that may elude detection with a manual search. X-ray machines are a common and practical mitigation effort for mail rooms and delivery docks, especially if the public is able to send packages or mail directly. Mail delivered hostile devices have become more common in recent decades, and every government department and agency should consider mitigation efforts to detect potentially hostile mail before it is introduced to a facility.

8.3. Checkpoint Planning and Operation

Employing checkpoints, either permanent or temporarily, should be considered when there is a concern, threat actors or prohibited items will enter a facility. Although they can be unpopular, they are often necessary when admitting people without security clearance, at mass gatherings, or when a site with cultural or political symbolism. All of these factors contribute to the risk of being targeted by threat actors. A TRA should be conducted to determine what items should be prohibited and the actions the security team should take if any are identified. Some items to consider prohibiting are:

- Mass casualty devices;
- Weapons;
- Intoxicants;
- Propaganda;
- Vandalism paraphernalia;
- Tools; and,
- Surveillance equipment.

SOPs should be in place that clearly outline how security staff are to respond to finding prohibited items; denial of entry, confiscations and even arrests. All guards working the checkpoint must be trained on these procedures and have clear directions on how to escalate and report any incidents.

9. Chemical Detection Equipment

Chemical detection equipment (CDE) has the ability to identify chemical elements and compounds (even trace amounts) and alert an operator to their presence. These devices can be calibrated to detect a vast number of chemical elements and compounds which help operators to identify; narcotics, explosives, cutting agents, precursor chemicals, and chemical warfare agents. CDE is available in a number of configurations, many come pre-loaded with a library of known substances and the ability to upload more as required. CDE can collect samples from the air or directly by swabbing an area of interest and inserting the swab into the testing device.

CDE can be deployed to continuously monitor for harmful chemicals in areas that may be subject to accidental or intentional introduction, such as industrial sites or transportation hubs. Mobile chemical detection devices are employed by first responders to rapidly identify harmful substances, which can assist in mitigating incidents involving real or perceived chemical threats.

CDE can be employed at points of entry to screen for chemicals which may prompt a secondary search, a denial of entry etc. Screening often involves security personnel swabbing areas of interest (such as hands, shoes, bags, or electronic devices), or having a person walk through a portal, similar to a walk-through metal detector, to test for trace elements of chemicals. There should be an SOP in place to outline the response to the detection of various chemicals to properly mitigate the threat.

A TRA should be undertaken to account for particular threat environments or increased risk of the use of chemicals which can warrant the deployment of CDE, especially in cases where actual threats are indicated to determine which chemical detection system is best suited to mitigate and minimize the risks involved.

10. Security Considerations

Safeguards may have a simple cause and effect relation with risk when analyzed independently; in practice there are many variables that can affect these calculations which must be considered. Physical security considerations, having a direct effect on safeguards and safeguard efficiency, include the following:

10.1. Defense in Depth

Defense in depth, also known as rings of protection, is a concept that an asset should have multiple layers of security safeguards that become increasingly dense the nearer you get to an asset. A perimeter fence is the most common first layer of defense; it is effective at establishing where public access ends but will do little to delay a deliberate threat actor from breaching or scaling it. Common detection efforts in the second layer include CCTV systems, security guard patrols, motion sensors, and access control safeguards; these are likely to be effective against most unsophisticated threat actors. The inner layers will be the most stringent and difficult to breach and will likely include multiple physical security safeguards working together to protect the asset from being compromised. As well as being highly difficult to breach for even sophisticated threat actors, these final layers of defense should also be designed to mitigate the risk posed by insider threats who may use valid credentials to bypass the first defensive layers. These final layers will likely have strict asset control that limits access to specific staff with a need-to-know or need-to-access.

10.2. 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.

Before a person moves from one physical security zone to another, they should perceive the zoning boundary (implied or actual) and understand the rules or limitations associated with crossing it. Departmental functional space requirements should also be taken into consideration when establishing zoning boundaries.

For additional information on physical security zones refer to GCPSG-015 Guide to the Application of Physical Security Zones.

10.3. Protection, Detection, Response, and Recovery

PDRR are the four critical components that make up a dynamic and efficient security posture. Every safeguard or mitigation effort is designed to address one or more of these elements. Consult GCPSG-019 - Guide to Protection, Detection, Response, and Recovery for an in-depth look at these concepts.

10.3.1. Protection

Protection is achieved using physical, procedural, and psychological barriers to delay or deter unauthorized access. Appropriately selected and utilized safeguards will impede the occurrence of unwanted events or activities

10.3.2. Detection

Detection involves the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred. Safeguards supporting detection should enable the earliest possible notification of an event, in order to reduce the amount of time necessary to initiate a response.

10.3.3. Response

Response entails the implementation of measures to ensure that security incidents are dealt with as quickly and efficiently as possible, are being reported to appropriate security officials which ensures that immediate and long-term corrective action is taken in a timely fashion. Response priorities, in order, are:

1. Preservation of life and safety of personnel;
2. Safeguarding of GC information and assets; and
3. Protection of property to enable prompt recovery to normal operations.

Department and agency response plans and SOPs should be based upon a TRA that includes known and anticipated threats to the location and personnel, capabilities of onsite security personnel, and available support from First Responders (Police, Fire, Ambulance). These should be routinely practiced (exercised) by both security and non-security personnel in order to foster a greater awareness, preparedness, and enables an agile recovery to normal operations.

10.3.4. Recovery

Recovery refers to the restoration of full levels of service delivery following an incident. This can include evidence collection to assist in prosecution.

10.4. Crime Prevention Through Environmental Design (CPTED)

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention during the designation, definition, and security design of an environment. 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 behavior and activities while discouraging undesirable actions by staff, visitors, and potential adversaries.

11. System Selection and Zone Considerations

Physical security systems all benefit from the application of Defense in Depth and detection systems should be a part of each zone transition area with safeguards becoming increasingly comprehensive the closer they are to valuable assets. A TRA will provide information on the nature and severity of threats to a facility and should be conducted to assist in selecting appropriate detection systems to best suit the needs of the site. Zones to consider employing detection equipment are:

Table 2: Zones and Selection Recommendations

Zone	Recommendations
Public	• CCTV (Monitored) - Allows security teams to rapidly identify conditions in the public spaces on and around a facility, including but not limited to protests, civil unrest, harassment of approaching staff; • CCTV (Unmonitored) - Does not provide a detection element, however it can be used in post incident investigations and therefore should not be disregarded entirely; and • Vibration Detectors (fence) - Can be an effective way to alert security when there is an attempt to scale or otherwise breach a perimeter fence between a public area and controlled spaces where methods like motion detection would be unfeasible due to the proximity to public throughways.
Reception	• Motion/Tomographic Sensors - An effective way to detect when a person has entered the space when there may not be other detection elements present. A reception zone (RZ) is an area where visitors are expected, therefore it is good practice to limit alarms linked to the motion detection system to times in which visitors are not expected to be present; • Photoelectric Sensors - An effective way to compartmentalize areas where visitors and staff are separated within a RZ, such as behind the service desk. Sensors set up in this way will generally emit an audible alarm when activated, which will alert staff and act as a psychological deterrent; • Glass Break Sensors - Alert security in the event that a window is smashed, and would require immediate action regardless of the time of day; • Contact Alarms - Installed on doors and windows can alert security when one is opened outside of operational hours. Additionally, an audible alarm can be activated if a door is opened without properly authorization which, can alert staff and work as a psychological deterrent; • CCTV - Allows security teams to rapidly identify conditions in the RZ, and can provide evidence to assist in post incident investigations; • Checkpoint (visual monitoring) - This could be reception staff or dedicated security personnel. In either case, the staff member should be trained in security awareness and familiar with the internal procedures for alerting security or law enforcement should the need arise. At a checkpoint, access control is often required such as; sign-in sheets, ID checks/access cards, or assigning escorts for visitors; • Metal Detectors – If identified as a requirement, a metal detector may be permanently or temporary used to screen staff and visitors as they enter the facility. Metal detectors require SOPs and trained security staff to operate them; and • X-rays - Often used for scanning bags and containers coming into a facility when a physical search is inappropriate or otherwise ineffective. The use of an x-ray machine will often be implemented only if deemed necessary by a TRA. X-ray machines require SOPs and trained security staff to operate.

Operation	• Motion/Tomographic Sensors - An effective way to detect when a person has entered a space where there may not be other detection elements present. These systems can be set to only be active outside of operational hours to limit false alarms caused by staff on duty; • Glass Break Sensors - In cases where the operation zone has glass barriers between it and an RZ or public area, they will alert security in the event a window is smashed, an event that would require immediate intervention whether or not it occurs during or after operational hours; • Contact Alarms - Installed on doors and windows can alert security when one is opened without first scanning an access card/entering a pin, or when opened outside of operational hours; • Visual Monitoring - Properly trained and security aware staff can assist in site security by reporting when they see an individual in an OZ without the proper pass and/or escort. This should be a supplementary safeguard and should not be used in lieu of dedicated and formal security measures; • CCTV - Allows security teams to rapidly identify conditions, and can provide evidence to assist in post incident investigations; and • Patrols - Trained security staff can be an effective method to bolster the security profile of a site, they operate security equipment, and conduct patrols which increases the presence of the security team and allows them to rapidly respond to emergencies.
Security/ High Security	• Motion/Tomographic Sensors - An effective way to detect when a person has entered a space where there may not be other detection elements present. These systems can be set to only be active outside of operational hours to limit false alarms caused by staff on duty; • Contact Alarms - Installed on doors and windows can alert security when one is opened without first scanning an access card/entering a pin, or when opened outside of operational hours. In addition, they can be used to further compartmentalize assets within a zone by installing them on specific security containers, which can indicate when they have been accessed. In cases where the mechanism is electronic and not manual, an alarm can be sounded if the container is pried open without properly entering the PIN or scanning an access card; • CCTV – Allows security teams to rapidly identify conditions, and can provide evidence to assist in post incident investigations. In security zones (SZ) and high security zones (HSZ) considerations must be given to ensure CCTV does not look over areas where sensitive information is processed. Restrict surveillance to access points and travel routes; and • Patrols - Trained security staff can be an effective method to bolster the security profile of a site, they operate security equipment, and conduct patrols which increases the presence of the security team and allows them to rapidly respond to emergencies. Security staff must hold the security clearance equal to the highest level of sensitivity being processed in the zone they are patrolling.

In addition to analyzing each zone's detection requirements, considerations should be made for additional factors including but not limited to:

- Hours of operation;
- Easements;
- Shared spaces;
- Population density; and
- Delay/Response times.

These factors can change detection system requirements and also highlight complications which may affect the choice of detection equipment used. For example, a facility located in a highly populated area may not benefit from motion sensors on the perimeter in which pedestrians would cause constant alarms. In this case, a vibration sensor on the perimeter fence may be more effective as it would only alarm if someone attempted to scale the fence. Conducting a TRA is the most efficient way to accurately evaluate the specific needs of each site.

12. Conclusion

Detection systems are highly modular and customizable, with solutions that can be added or changed at various times depending on the situation faced. An understanding of the threat environment is as important as understanding the available detection devices to counter those threats. Once a threat has been identified, an appropriate detection system may be selected and implemented. Manufacturers of detection equipment can work with a department or agency's physical security team to identify a commercial-off-the-shelf or custom product to efficiently mitigate a range of risks a facility could face. Detection is an important consideration for the physical security and defense-in-depth of every facility.

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
- GCPSG-011 (2024) – Guide to Closed Circuit Television/Closed Circuit Video Equipment Systems
- GCPSG-019 (2023) – Protection, Detection, Response, and Recovery Guide
- The International Crime Prevention Through Environmental Design Association
- Harmonized Threat and Risk Assessment (TRA) Methodology

14. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-021 (2025) – Fundamentals of Detection Systems in Physical Security, for approval.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2025.04.25 14:05:25 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby recommend, GCPSG-021 (2025) – Fundamentals of Detection Systems in Physical Security, for approval.

St-Pierre,Andre
Vincent,000171484

Digitally signed by St-Pierre,Andre
Vincent,000171484
Date: 2025.05.20 11:09:05 -04'00'

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

Date