Guide to Closed Circuit Television/Closed Circuit Video Equipment Systems

GCPSG-011 (2024)

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

Publication Issued: 2024-05-15
Updated: YYYY-MM-DD

Foreword

The Guide to Closed Circuit Television (CCTV) / Closed Circuit Video Equipment (CCVE) Systems 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 the design and the implementation of a CCTV/CCVE System 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-011 – Guide to CCTV/CCVE Systems is 2024-05-15

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. This includes the guidelines for Closed-Circuit Television/Closed-Circuit Video Equipment (CCTV/CCVE) Systems at GC buildings and facilities.

Note: hereinafter the use of CCTV in this guide will be understood to include CCTV and CCVE systems.

1.1. Purpose

The purpose of this guide is to provide GC security professionals with information on the appropriate design, selection, and procurement of CCTV systems and components as part of a facility's overall security posture including; access management and protection, detection, response, and recovery processes.

The guide contains both required security control safeguards, indicated by use of the word "must" and recommended security control safeguards or guidance, indicated by the use of the word "should". Use of the word "must" indicates a reference to an established GC policy or standard, while the use of the word "should", refers to advice, guidance or a best practice.

Baseline physical security measures are designed to provide protection against common types of threats that departments and agencies may encounter. Certain departments and agencies or operational activities may face different threats because of the nature of their business, their location, or the attractiveness of their assets. Examples include police or military establishments, health services, laboratories, sensitive research facilities, museums, service counters, offices in high-crime areas and facilities located outside of Canada.

1.2. Applicability

This guide applies to GC employees and contractors with responsibilities in the security and property management of GC facilities. This includes personnel involved in the design of facility surveillance systems, Chief Security Officers and delegated managers for security and facility management, and security practitioners responsible for conducting Threat and Risk Assessments (TRA) and implementing mitigation measures.

GC departments and agencies are responsible for determining their security requirements for site selection and facility fit-up and the security safeguards considered necessary to protect facilities based on a Threat and Risk Assessment (TRA). This responsibility includes measures for security (exterior doors, CCTV, and security lighting), building systems (mechanical and electrical systems) and life safety (exit stairs, fire alarms and sprinklers). CCTV requirements fall under this responsibility.

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

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

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

Departments and agencies should conduct a risk management exercise to ensure, that while the dignity of all is respected, the protection of GC information, assets, and personnel is maintained. All questions on EDI policies and directives should first be addressed to your responsible departmental authority.

1.4. Information Technology Considerations

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

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components 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
AHJ	Authority Having Jurisdiction
CCTV	Closed Circuit Television – includes related video equipment
CCVE	Closed Circuit Video Equipment
DSM	Directive on Security Management
DVR	Digital Video Recorder
IP	Internet Protocol
LED	Light Emitting Diode
ONVIF	Open Network Video Interface Forum
PGS	Policy on Government Security
PSIA	Physical Security Interoperability Alliance
PTZ	Pan – Tilt – Zoom
RCMP LSA	RCMP Lead Security Agency for Physical Security
SA&A	Security Assessment and Authorization
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment
UPS	Uninterrupted Power Supply

4. Glossary

Term	Definition
Closed Circuit Television	Any electronic surveillance system consisting of cameras, monitors, recording equipment, and other technologies to monitor any space.
Closed Circuit Video Equipment	Any components of an electronic surveillance system consisting of cameras, monitors, recording equipment, and other technologies to monitor any space. Interchangeable with CCTV.
Collateral Signal Interference	Any unintentional disruption of wireless communications signals by other frequency signals present in the operating area.
Electronic Intrusion Detection (EID)	A system consisting of sensors that detect a change in state (motion, electric current, heat, passcodes, etc.), conveys messages to an electronic monitoring program or notification equipment (alarm bell, switchboard, remote access software, etc.), and permits analysis of the reported change in state (audible alarm, Security Operations Centre, call-tree/electronic notification, etc.).
Force Multiplier	Any action, training, resource, or tool that increases the effect or effectiveness of an action, process, or system.
Open Network Video Interface Forum	An industry forum facilitating the development and use of a global open standard for the interface of physical IP-based security products and for how IP products within video surveillance and other physical security areas can communicate with each other.

Physical Security Interoperability Alliance	A global group of physical security manufacturers and systems integrators promoting interoperability of IP-enabled security devices and systems in physical security and promote and develop open specifications, relevant to networked physical security technology, across all industry segments including video, storage, analytics, intrusion, and access control.
Threat Risk Assessment (TRA)	Assessment of a facility to identify risk, threats and vulnerabilities to assets (information, employees, services, etc.).

5. Introduction to Closed-Circuit Television Systems

The ability to detect and respond to emergencies or security events depend largely on the capability to continuously monitor an area or space. In addition, the ability to coordinate a response to counter any activity that threatens the safety and security of people or property is dependent on reliable, clear, and timely information. The use of human-only surveillance, though effective and highly adaptable if properly trained, is costly in terms of financial and oversight resources. Additionally, human surveillance may be tainted by personal perceptions, bias, training shortfalls, and external influence. Electronic surveillance methods have proven to be more effective at providing an unbiased, visual record of events for responding security personnel or first responders.

Originally designed as a network of cameras linked to one or more television monitors to provide a real-time, remote monitoring capability, CCTV has evolved with technological advancements in audio-visual quality, wired and wireless signals, and digital imagery and storage. Today remote video surveillance products are available in a wide variety of applications and capabilities resulting in a wide variety of terminology. For ease of understanding, in addition to the note in Section 1, the term CCTV shall be used in this guidance to describe any electronic surveillance system consisting of cameras, monitors, recording equipment, and other technologies to monitor any space. Departments and agencies may use terminology that suits their unique needs although the acronym CCTV is highly recognizable and interchangeable with many modern products and systems.

5.1. Protection, Detection, Response, and Recovery

It is important to note that CCTV does not prevent intrusions, criminal activities, state-sponsored or corporate espionage, or violent incidents from occurring in or near GC facilities. CCTV systems should not be employed for the purpose of monitoring employee performance or attendance as this practice would be contrary to provisions within the Privacy Act which advises video recordings and images contain personal information and disclosure of CCTV recordings for an administrative purpose would require the individual's consent. Departments and agencies should utilize CCTV as an enabling technology in access management and their protection, detection, response, and recovery efforts. CCTV should be employed in co-operation with additional security measures and procedures.

5.1.1. Protection

A well designed and maintained CCTV system is a force multiplier that enables departments and agencies to continuously monitor areas that would not be possible by a security force alone. CCTV is limited as a physical protective measure. The presence of CCTV cameras may act as a psychological barrier, or deterrent, against intrusion.

5.1.2. Detection

CCTV systems enable security personnel to monitor areas devoid of personnel, access management locations, establish baseline patterns of movement in and out of an area or facility, identify an attempted intrusion, and initiate a response. Limitations of CCTV systems in detecting intrusions are commonly caused by poor or insufficient camera coverage of the space ("blind spots"), inadequate number of personnel to effectively monitor all cameras, or a lack of training on the provided equipment. Therefore, it is important to maintain a proper Access Management System.

5.1.3. Response

The use of live CCTV imagery to coordinate a response, by security or law enforcement personnel is an effective method to limit the impact or damage to personnel, property, information, or public reputation of the GC. Ideally, the CCTV system should be monitored and controlled within, or immediately adjacent to, a Security Operations Centre and supported by a reliable communications system. This should allow for live monitoring and recording of an active event without interfering with the ongoing viewing of other live cameras.

5.1.4. Recovery

In order to enable a rapid return to normal operations or service delivery, Security Operations Centre personnel may use the live CCTV video to coordinate recovery efforts until additional personnel are available. More information on responding to emergency events is available from Public Safety Canada.

6. Design Considerations

The design of any CCTV system should be based on a properly conducted Threat and Risk Assessment (TRA) in order to identify site-specific requirements, vulnerabilities in current physical security measures, and future needs or plans for the facility. Additional considerations for custodial departments, agencies, and multi-tenant facilities will be identified in the TRA process. Representatives from the Safety, Security, Property Management, Maintenance, Information Technology (IT) and Human Resources teams should be consulted during the design phase before a CCTV system is selected. It would be very helpful to engage the services of a professional CCTV design architect/firm during the design phase of any project.

6.1. Establish Requirements

When establishing CCTV requirements, based on safety and security vulnerabilities identified in the TRA, key areas of concern may include:

- **What areas need 24/7 observation?** Areas may include parking facilities, perimeter border(s) of the property, entrances and exits of the facility buildings, and reception areas. Is sensitive information safeguarded from view or recording of the CCTV;
- **Why is CCTV needed or preferable for the identified areas?** History of criminal activities or safety concerns, area is too large to fully surveil solely using security personnel, or other reasons identified in the TRA;
- **How is the CCTV system to be used?** Are there operational or legal considerations that require a continuous surveillance or record of the environment? Has a Privacy Impact Assessment (PIA) been completed or is one needed;
- **Are there any legal requirements?** The posting of signage to notify CCTV systems are employed can be a requirement. Each location has unique requirements, under law, and the Authority Having Jurisdiction (AHJ) sets what is required for signage; and
- **Where and by whom is the CCTV system to be monitored, controlled, and maintained?** On-site or remote monitoring of CCTV imagery, use of a Security Operations Centre or a contracted security service, or integrated with an access management system or intrusion alarm devices?

6.2. Identify Constraints and Limitations

In addition to the CCTV requirements established to counter or manage vulnerabilities identified during the TRA process, departments and agencies should also factor existing limitations into the design of a CCTV system.

6.2.1. Lighting

Departments and agencies should have security lighting employed in line with GCPSG-004 (2020) Security Lighting Considerations Guide; as this will aid most CCTV systems in properly capturing imagery for viewing. Ensure the coverage areas are assessed during lowlight and night-time conditions to determine if additional lighting is needed or if selecting cameras capable of viewing and analyzing imagery in these conditions is required. For example, access areas located on the East or West side of a facility will have special considerations for sunrise and sunset; as cameras facing the rising or setting sun will have obscured imagery caused by bright light, shadows, and moisture changes inside the camera housing (fogging or ice). An alternate camera location or angle may be necessary to avoid this type of obstructed view if the camera is not equipped with technology to adjust to these conditions.

6.2.2. Infrastructure

Is the CCTV system a new installation or replacing an existing system? Departments and agencies should evaluate the existing CCTV against the identified requirements to ensure an inadequate design is not being copied or reused to keep costs low; the vulnerability

will still exist with the new equipment or architecture. Similarly, the same applies to the CCTV control systems in a Security Operations Centre.

6.2.3. Environment

Canada's climate varies greatly throughout the year. CCTV systems need to be effective in the extreme range of temperatures and weather conditions of the employed location. For example, camera housings should be highly resistive to moisture entering causing ice or fogging that would impede the effectiveness of the camera lens. High winds, rain, and snowstorms can disable wireless communications if the antenna(s) are not designed for this environmental factor. Trees and other vegetation may impede camera views at time of installation or later as they continue to grow. Special care to select CCTV components that can survive and function properly in the location's climate is necessary to avoid loss of coverage and frequent or unnecessary repairs and replacement.

6.2.4. Power Supply

The CCTV components must be compatible with the electrical supply of the location. Components sourced from outside the country may not have the same input voltage as the electrical supply at the site. Best practice is to verify all components of the system meet local standards; such as, 100 – 240V ratings. Other power supply considerations may include, back-up power supply, such as generators or Uninterrupted Power Supply (UPS), or the use of alternative energy sources, including solar power with battery back-up, as potential electrical power supply options for new projects or renovations.

6.2.5. Capability to Expand

CCTV requirements may change over time. When designing a CCTV system, considerations should be made towards using a technology platform that is compatible with components from multiple manufacturers and is capable of future expansion or alteration. Having a CCTV system that is modular in design and can more easily be modified to adapt to new configurations may reduce future vulnerabilities and costs.

6.2.6. Serviceability

The availability of replacement parts and licenced technicians to maintain the system should be a consideration when selecting a CCTV system and maintenance contract. Any delay in repairing a non-functional CCTV component increases the vulnerability and risk of exploitation.

6.3. Interoperability

Physical security systems are intended to work in a complementary fashion in order to provide a robust mitigation of security risks faced by departments and agencies. Whether expanding an existing CCTV system or designing a new one, the ability of the selected CCTV components to integrate with other technologies and processes should be a consideration.

6.3.1. Electronic Intrusion Detection

The integration of CCTV with a facility's intrusion detection system may facilitate a rapid evaluation of any alarm and aid responding personnel in the coordination of their investigation. For example, CCTV systems employing Pan-Tilt-Zoom (PTZ) cameras could be triggered by sensors (motion detector, window or door contacts, panic button) to immediately direct one or more cameras towards the triggered sensor for a rapid visual survey of the alarm area so long as there is redundant coverage of the area(s) the PTZ viewed prior to the alarm.

6.3.2. Access Management Systems

Similar to an integrated CCTV and Electronic Intrusion Detection system, the use of CCTV to support Access Management systems would be an advantage if a facility has an identified risk of perimeter breaches or forced entry identified in a TRA. The ability to identify and track persons or objects before they have breached a perimeter fence or entered a facility could allow security personnel to coordinate activities to disrupt or intercept the would-be intruder.

6.3.3. Building Management Systems and Infrastructure

Building automation and CCTV integration may optimize the monitoring of critical infrastructure such as heating, ventilation, and cooling (HVAC) systems, power generation equipment, hazardous material storage areas, or other locations that may not have a constant human presence. If permitted by the security categorization of the area being monitored, remote surveillance of these systems may be possible in a facility's Security Operations Centre, CCTV Command Centre, or via an Internet Protocol Network or software.

6.3.4. Standards for Interoperability of Internet Protocol Technology

Internet Protocol based systems, or IP, have the capability to provide high-performance video in a cost-effective manner. Due to the popularity of this technology, it is vital that IP components, within a CCTV system, are capable of operating with the entire network. Standards for this interoperability include:

- Open Network Video Interface Forum (ONVIF), an established standard for the communication of video surveillance between IP products; and
- Physical Security Interoperability Alliance (PSIA), an established standard of specifications for IP-enabled security devices and systems; including video, storage, analytics, intrusion detection, and access management.

As noted in 6.2.5., the capability to expand an existing or future CCTV system is largely dependent on the interoperability of the system components. Departments and agencies should verify their CCTV systems have this capability to expand or should factor in the scalability and interoperability of the components in the design of new CCTV system.

7. Components of a CCTV System

CCTV systems are a connected network of equipment designed to capture, transmit, display, and store imagery data. CCTV systems range in complexity from a single camera connected to a monitor, displaying the video images, up to networked systems capable of monitoring and controlling hundreds of cameras connected locally, remotely, and globally. See Appendix A – Technological Considerations to view a comparison of the technological advancements in CCTV components. The common components of a CCTV system are:

7.1. Cameras

The most recognizable, public-facing component of a CCTV system, cameras are the sensors that convert the visible scene formed by the lens into an electrical or binary signal suitable for transmission to a remote device. Selecting the appropriate camera needed for the environment, application, and available infrastructure is extremely important. Due to the rapid advancement in technology, departments and agencies should be mindful of future compatibility and functionality when selecting CCTV cameras.

7.1.1. Camera Types

See Appendix A – Technological Considerations to view a comparison of Analog, Digital, and Digital IP technologies when evaluating the type(s) of camera needed for a location's CCTV. Categorized by function, but often designed with overlapping capabilities, camera types available for departments and agencies include:

- **Fixed Camera:** These cameras are mounted in a stationary position with the purpose of focusing on a primary field of view or area of interest. Located both indoors and outdoors, overtly or covertly, and vary in size and durability. Commonly used for 24/7 monitoring of perimeter fencing and open spaces; however, these cameras are limited in providing a "full picture" if other cameras do not provide an overlapping field of view to prevent "blind spots". These cameras can be integrated with intrusion detection systems with the appropriate software and/or proper labelling of the camera view on the connected monitor;
- **Pan-Tilt-Zoom Camera:** Pan-Tilt-Zoom (PTZ) cameras allow the camera to be moved remotely, via a controller, to the left or right (panning), up and down (tilting), and allow the lens to zoom in and out. These cameras are best utilized with security personnel operating the CCTV system in a control room or Security Operations Centre. PTZ cameras have the advantage of allowing the operator to track a moving person or locate a suspicious item for remote observation. Standard operating procedures should be established, following any change of view, to ensure a PTZ camera is returned to the original field of view if it is being used primarily for a static observation. PTZ cameras may also have a "patrol" function to "sweep" areas instead of remaining in a static position;
- **Dome camera:** Can function as a fixed or PTZ camera concealed in the dome-shaped housing. The outer casing of the camera housing makes it difficult for onlookers to identify which way the camera is facing and may provide some

deterrence against undesirable or criminal activities. The housing of dome cameras may also include vandal-resistant features. Dome cameras are used for both indoor and outdoor surveillance and are well suited for entrances, stairwells, reception lobbies, and security screening areas;

- **Bullet Camera:** A more robust version of the fixed camera, bullet cameras are cylindrical, are manufactured in a variety of lengths, and are ideal for outdoor use. Installed within protective casings, the cameras are shielded from dust, dirt, and other natural elements. They come fitted with different lenses depending on the requirements of the application, including some bullet cameras that have small LED lights surrounding the lens to detect moving figures in lowlight or night conditions;
- **Day/Night Camera:** Capable of operating in poorly lit environments or outdoor locations. These cameras are equipped with an extra sensitive imaging chip that enables a viable image automatically in changing, lowlight to bright, conditions;
- **Infrared/Night Vision Camera:** Similar to day/night cameras, infrared/night vision cameras can be either a fixed or PTZ camera and are equipped to capture imagery in lowlight to night-time conditions. The effectiveness of these cameras will depend on the capability of the installed lens and imagery sensor(s). This type of camera is advantageous for 24/7 monitoring of vital infrastructure; such as airports, seaports, power generation facilities, other critical infrastructure, and overseas diplomatic or defence facilities; and
- **Thermal Imaging Camera:** A thermal camera captures and creates an image of an object by using infrared radiation, or heat, emitted from the object that is invisible to the human eye. Thermal image cameras are capable of detecting heat or infrared signatures over long distances with specialized infrared emitters; however, thermal imagers are not effective at detecting through glass or water. There is some limited ability to provide an image through low-density smoke or fog but the thermal sensors can degrade over time and may require more frequent maintenance or replacement.

7.2. Lenses

A camera lens is a piece of glass or plastic designed to control and focus the amount of light from the outside world onto the imaging sensor within the camera; creating a clear image(s) of the scene at the correct exposure. There are three basic lens types for CCTV cameras – fixed, varifocal and zoom and these can include design options for low-light conditions.

7.2.1. Types of Lenses

Each type of lens has characteristics that differ from the others, depending on the intended application, and provide the best possible image and detail for the area being monitored. These characteristics include:

- **Fixed Lens:** Fixed lenses have a set focal length and horizontal field of view that requires the camera to be physically moved closer or further from the monitored area to alter the amount of detail that can be viewed. Fixed lenses work well in a

general observation application monitoring a small area, such as a reception lobby or entrance door;

- **Varifocal Lens:** Varifocal lenses typically provide more flexibility with installation positions due to the range of focal lengths in the lens that provide different fields of view. Varifocal lenses still require manual adjustment for altering the field of view;
- **Zoom Lens:** Similar to the varifocal lenses' designed ability to change the field of view for a camera, zoom lenses allow for remote alteration of the focal point but with a greater range of the field of view than the other lens types. Motorized zoom lenses have the benefit of refocusing the field of view as the lens is adjusted by an operator; and
- **Auto-Iris or Aspherical Lens:** An additional consideration in lens selection may include the light conditions of the environment under view. In an auto-iris lens, the camera controls the opening and closing of the iris in the lens; depending on how much light is required in order to produce an image. Aspherical lenses are designed with a more convex shape than a normal lens to gather more light and allow for a better image in inconsistent light conditions. These lenses are available in a variety of shapes and can correct for light focusing at different points, called spherical aberration, as the light passes through the lens. This can aid in producing a better picture in lowlight applications.

7.3. Camera Housing and Mounts

CCTV cameras can be delicate pieces of equipment that require protection from physical interference and environmental conditions. Selecting the appropriate protective housing and mounting hardware differs for exterior and interior cameras in a CCTV system. Consideration towards environmental conditions for cameras located outdoors is of importance. Extreme heat and cold can be damaging to electrical devices as are wet and dry or dusty climates. Ensuring the appropriate camera housing and mounting hardware is employed will help to protect CCTV cameras and enable optimal conditions for imagery collection.

7.3.1. Camera Housing

The protective shell, or housing, of a CCTV camera should be matched to the type and function of the camera and the environment for which the camera is located. Attention should be paid to the housing's ability to withstand moisture, significant temperature changes, physical impact, and foreign particulates from interfering with the camera or the imagery captured. Examples of camera housings include:

- **Sealed Housings:** designed to prevent contamination (water, dust, chemical vapours) from the outside environment from damaging the electrical components of the camera;
- **Impact-Resistant Housings:** constructed of robust materials, this housing type is designed to withstand physical interference from vandalism and violent offenders;
- **Tamper-Resistant Housings:** similar to impact-resistant models, these are

constructed of hardened outer shells but permit access to the camera via a lockable port. These models are designed to resist forcible entry;
- **Dome Housings:** frequently used with PTZ cameras, these "domes" conceal the direction the camera is facing and are less obvious to outside observers. Additionally, the low profile of the dome shape limits interference from environmental conditions (wind, rain, snow) that can cause vibration; and
- **Bullet or Blast Resistant Housings:** constructed with high impact-resistant materials to limit the effect of violent impact from blast or firearms. This type of housing would normally be limited to military and diplomatic facilities in hostile environments.

7.3.2. Camera Mounts

CCTV cameras can be mounted to a wide variety of surfaces when designing the camera layout of a CCTV system. As with the camera housing, the mounting hardware will depend upon the camera functions, intended use, and the environment for which it is located. Regardless if the camera is intended to be covert or overt, or located in an indoor or outdoor environment, common considerations are:

- **Size and weight of the camera:** both the hardware and material anchoring the mount, housing, and camera, must be able to withstand the combined weight;
- **Durability of Hardware:** the robustness of the mounting hardware and camera housing should be sufficient to protect the camera for the intended environment;
- **Field of View**: the camera should be mounted in a location that is capable of capturing/viewing the entire space intended, if an additional camera is not providing an overlapping field of view to observe the full space; and
- **Vulnerability to Tampering or Damage**: most CCTV camera locations should be out of reach to the general public. Mounting CCTV cameras in ceiling corners, on top of building structures, or on top of security lighting poles will limit the opportunity to damage or tamper with the cameras.

7.4. Monitors

Intended for the display of imagery captured by the network of cameras, CCTV monitors vary in image quality, size, and connectivity to other devices. The selection of monitor to use in a CCTV system should include considerations on the quality of image the monitor can produce, the durability of the monitor screen to continuous or prolonged operation (image burned into screen), power consumption/heat generated, the lifespan of the monitor or technological compatibility (analog vs digital/digital IP), and network transmission type (wired or wireless). The types of monitors available for CCTV systems may include:

- **Televisions**: standard, High Definition (HDTV), or Ultra High Definition (UHD). These can be dual purpose and have become common in many applications but can be susceptible to screen damage from prolonged or continuous use;
- **Computer Monitors**: normally connected to CCTV management and storage devices (Digital Video Recorder/DVR), this style of monitor works well in a workstation configuration in a CCTV control room or Security Operations Centre;

- **LCD/OLED Monitors**: Liquid-Crystal Display (LCD) and Organic Light-Emitting Diode (OLED) monitors are emerging as viable options, as CCTV monitors, due to increased availability and advancements in imagery technology. These come in a variety of sizes, are relatively lightweight (wall mounting), and require less electricity than previous technologies; and
- **Video Walls**: a networked collection of wall-mounted monitors, video walls work well in a Security Operations Centre setting and are capable of displaying a wide range of CCTV imagery and other video displays for facility layout and maps, alarms, event logs, and other applications useful in a situation requiring coordination or a security response.

Older CCTV systems employing more cameras than monitors will need to employ devices (such as switchers or mulitplexers) to allow the view displayed on the monitor to change from one camera feed to another. Digital and digital IP network systems do not require this extra hardware to alter the monitor's display.

7.5. Transmission Medium

The method of transmitting the video signals from the camera(s) to the system's processing device such as; the DVR or the monitors, is as important as the selection and quality of the camera, lens, and processing device. Ensuring a strong video signal across the entire network will enable a superior image that is available to the personnel watching the monitor. The transmission mediums can be divided into wired and wireless systems. Refer to Appendix A – Technological Considerations for a comparison of these video transmission mediums in the existing technologies.

7.5.1. Wired

The traditional method of transmitting video signals from camera to monitor, CCTV wiring technology has evolved significantly. Commonly available types for CCTV systems are Coaxial and Fiber-Optic cables. More specialized wiring options are available. Departments and agencies should jointly consult a video surveillance system designer and the departmental security authority on a case-by-case basis if specialized needs are identified in the TRA.

Coaxial cables have been the common connection in CCTV systems for decades. A multilayered cable, coaxial cable must have a copper core to properly transmit the electrical signal from the camera to monitor and a braided, 95% copper shield or mesh layer to limit external interference. If the length of cable is great, departments and agencies should employ amplifiers to ensure a strong signal throughout the network. As an electrical transmission medium, ensure coaxial cables are properly grounded to avoid signal disruption.

Fibre optic cables are composed of glass or plastic fibres wrapped in a protective layer. Unlike coaxial cables, fibre-optic cables transmit light pulses instead of electrical signals.

This requires the use of converters on both ends of the fibre-optic cables to convert the electricity to light pulses and back to electric signals. Although fibre-optic cable is more fragile and requires additional processing than coaxial cable, it is not affected by radio frequency nor electromagnetic interference and can transmit over significantly longer distances without the signal degrading.

7.5.2. Wireless

Wireless CCTV systems are very popular in residential and small business locations. The ability to establish and manage an entire CCTV system, without the infrastructure needed for a wired system, may provide a great deal of mobility and flexibility. Unfortunately, obtaining a dedicated frequency for transmissions may be difficult in some locations.

Wireless systems are more vulnerable to intentional or collateral signal interference and interruptions than wired systems. The increased instances of cyber-based interference and covert monitoring may be problematic for use in the GC. Departments and agencies should include these considerations, when conducting a TRA, before installing wireless components in the CCTV system.

7.6. Imagery Storage

CCTV recordings can be vital in the collection of evidence during investigations into criminal acts or critical incidents. Imagery storage has evolved greatly from tape-based to digital hard drives to internet cloud-based systems. Departments and agencies should evaluate their imagery storage needs, as part of a TRA, when designing or upgrading a CCTV system. Use of "in-camera/onboard" storage should be avoided due to the risk of tampering or unauthorized access especially for cameras located outside of a controlled area.

Digital Video Recorders (DVR) can offer customization in how imagery is recorded, what information is included in the display of the imagery, and which camera(s) are recorded. Options allowing continuous recording of imagery, with an overwrite setting (record over older footage), can save space on a hard drive. Many DVR systems are scalable and allow for many hard drives to work co-operatively to provide months to years of recordings if this capability is warranted. An added feature of removable hard drives is they offer flexibility in preserving original recordings for later use or as evidence if needed.

Network Video Recorders (NVR) are an IP-based system that stores video data and imagery transmitted via an internet network. These recording systems transfer the imagery and data to a storage drive or device (portable or mass storage) or to a "cloud-based" storage in a remote network server. This storage option may alleviate the need for physical storage in the CCTV control room or Security Operations Centre however, the imagery and data must be stored in a GC departmental server or an appropriately security screened and safeguarded location within Canada only. See 7.8.1. Cyber Security Considerations for more information.

Recorded imagery must be safeguarded in the same manner as other GC information. If unauthorized release of recorded imagery may be injurious, then those images would hold a categorization level equal to the potential level of injury. Consult DSM, Appendix J: Standard on Security Categorization and GCPSG-007 (2022) Transport, Transmittal and Storage of Protected and Classified Material for more information.

7.7. System Management

CCTV systems are often complex with a vast range of potential configurations to meet the needs addressed in a TRA. Departments and agencies can benefit by developing CCTV systems that are integrated with compatible hardware, software, infrastructure, and communications devices that promote interoperability and common understanding and maintenance of the system.

7.8. Internet Protocol Network Systems

Internet-based CCTV systems have been steadily replacing older analog systems largely due to the added benefit of interoperability with devices or computers networked anywhere in the world. With Power over Ethernet (PoE) technology, networked devices receive electrical power and transmit data via the same cable reducing the number of components needed and increasing efficiency in design. The capability to interact with multiple applications in a departmental access management system or Security Operations Centre increases the effectiveness of security personnel and allows for future expansion of a CCTV network.

7.8.1. Cyber Security Considerations

As with all internet-based applications, IP CCTV systems are vulnerable to cyber attack and covert monitoring if appropriate measures are not employed. Protection of the CCTV imagery should be regarded in the same manner as other sensitive information for the GC. Departments and agencies should consider using a Private Area Network for IP CCTV systems. This would provide an additional safeguard against unauthorized access to the CCTV system via a computer on the regular office network. For additional information or consultation on cyber security risks contact the Canadian Centre for Cyber Security.

8. Lifecycle Considerations

Regularly scheduled maintenance can enable CCTV hardware and software to operate efficiently, extend the service life of the equipment, and identify issues before a failure occurs. Preventative maintenance tasks may include:

- Visual inspection of the equipment for damage, discolouration, leaks, moisture (fogging), or corrosion;
- Checking for signs of unauthorized opening or tampering of the system components (tamper seals may be appropriate if this is an identified threat for the location);
- Cleaning cameras, lenses, and housings. Exterior cameras may require additional checks and cleaning when impacted by weather conditions;
- Completing the diagnostic testing recommended by the manufacturer(s); and

- Operating and testing all components, software features, and recording storage quality of the CCTV system.

As a CCTV system, or any key component within the system, is nearing the end of the expected service life, departments and agencies should evaluate the feasibility of repair or replacement against the longer-term effectiveness of the entire CCTV system. A CCTV system in a constant state of disrepair or near-collapse is an increased vulnerability that aggravates risks identified in a TRA. Departments and agencies should consider replacing obsolete or disjointed CCTV components with a comprehensive or compatible CCTV system that is designed to meet the needs, and potential future needs, identified in a TRA.

Service agreements and maintenance contracts may include emergency "call-out" (defined response times), 24-hour care, and warranty and non-warranty repairs. Departments and agencies may assess the need to retain replacement CCTV components and equipment on-site to avoid prolonged delays in restoring full functionality of the system.

9. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Privacy Act
- Communications Security Establishment (cse-cst.gc.ca)
- Canadian Centre for Cyber Security
- Public Safety Canada
- Office of the Privacy Commissioner of Canada - Surveillance
- Privacy Act: Plain Language Guide to Exemptions and Exclusions - Canada.ca
- CCTV Technology Handbook, July 2013, US Department of Homeland Security
- CCTV, March 2022, UK National Protective Security Authority
- Directive on the Duty to Accommodate
- Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service
- Guide for Two-Spirit, Transgender, Non-Binary, and Gender-Diverse Employees
- Open Network Video Interface Forum
- Physical Security Interoperability Alliance
- GCPSG-003 (2021) Security Operations Centre Design Considerations Guide
- GCPSG-004 (2020) Security Lighting Considerations Guide
- GCPSG-006 (2024) Access Management Guide
- GCPSG-007 (2022) Transport, Transmittal and Storage of Protected and Classified Material
- GCPSG-019 (2023) Protection, Detection, Response, and Recovery Guide
- GCPSG-022 (2024) Threat and Risk Assessment Guide

Appendix A – Technological Considerations

Specifications	Analog	Digital	Digital IP
Video Quality	Good in low light but poor or degraded/ graining images when expanding for zoom in features	Higher quality than Analog with better zoom/imagery versatility	High Definition Digital with superior video detail and greater sight range. Wider viewing field and higher detail available in zoom functions
Resolution	720 x 480 pixels	1280 x 720 pixels to 8 megapixels (3840 x 2160)	Up to 8K UHD (7680 x 4320) compressed, encoded transmissions.
Power Supply	Cameras require separate power source/electrical wire to operate	Cameras require separate power source/electrical wire to operate	Power over Ethernet capable. Removes need for separate electrical wire to power cameras.
Transmission Medium	Wire or Coaxial Cable (must be copper)	Coaxial Cable (copper core) or Fibre Optic	Ethernet and Wireless
Wired/Wireless	Wired	Wired	Both. Practical solution in areas difficult or expensive to run cable; such as in historical buildings. Emission Security should be factored into the decision-making process. Contact CSE for guidance on signal emissions security.
Signal Transmission Distance	Can transmit video signal up to approximately 1.5 kms via traditional twisted-pair wired cable or 600 metres via coaxial cable.	Can transmit video signal approximately 600 metres via coaxial cable or 950-1000 meters via fibre-optic cable	IP cameras can send digital video 100 metres over twisted-pair Ethernet cable and unlimited distances over IP networks. Images maintain 100% clarity over long distances and when the signal is converted between different formats.
Signal Transmission Security	Requires very close or physical access to breach or intercept imagery or emitted electrical signals.	Coaxial cable same as Analog. Fibre Optic is less vulnerable to radio frequency and electromagnetic	Signal transmitted as internet data; both wired and wireless. Same security concerns

	Cannot be remotely accessed as it is not connected to the internet.	interference but is fragile compared to coaxial cable.	as internet and mobile data signals.
Reliability	Vulnerable to radio frequency and electromagnetic interference.	Coaxial cable same as Analog. Fibre Optic is less vulnerable to radio frequency and electromagnetic interference but is fragile compared to coaxial cable.	Vulnerability tied to internet network and external interference (hack, ransomware, operating system). Software compatibility is a concern.
Ability to Expand System	Expansion requires added infrastructure to accommodate cabling.	Expansion requires added infrastructure to accommodate cabling.	Expansion integrates easily into existing network with additional licenses for software
Ease of Installation	Requires standard infrastructure (conduit) to power and link network). Larger networks need more support.	Requires standard infrastructure (conduit) to power and link network). Larger networks need more support.	Less infrastructure needed than non-IP systems.

10. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-011 (2024) – Guide to CCTV/CCVE Systems, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.05.13 10:26:35 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby recommend, GCPSG-011 (2024) – Guide to CCTV/CCVE Systems, for approval.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.05.23 12:05:22 -04'00'

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

Date