Transport, Transmittal and Storage of Protected and Classified Material

GCPSG-007 (2022)

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

Publication Issued: 2022-10-13
Updated:

Foreword

The GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material Guide is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA). Although UNCLASSIFIED, access to and use of this guide should be limited to Government of Canada (GC) departments and agencies.

Reproduction

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

Effective Date

The effective date of the Transport, Transmittal and Storage of Protected and Classified Material Guide is 2022-10-13.

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

1.1. Purpose

In accordance with the Treasury Board Secretariat's (TBS) Directive on Security Management (DSM), departments must protect against the unauthorized disclosure of protected and classified material shared between Government of Canada (GC) and other governments (including foreign, provincial, territorial & municipal), international, educational and private organizations.

This guide provides guidelines in order to ensure appropriate protection against unauthorized observation, modification, or disclosure (deliberate or inadvertent). The guide contains both minimum requirements and recommended safeguards. Use of the words "shall" or "must" indicates a requirement. Use of the word "should" indicates the recommended safeguards. A TRA may indicate additional security measures are necessary.

NOTE: the use of the word "Material" throughout this guide includes all information or assets.

1.2. Applicability

This guide applies to staff of all GC departments and agencies who Transport, Transmit or Store protected and classified material. Each departmental Chief Security Officer (CSO) should determine the necessity of alternative or additional safeguards above the minimum recommended, based upon a Threat and Risk Assessment (TRA) or Security Assessment of known or heightened threats.

This guide provides direction and guidance for the transport and transmittal of protected and classified material (on paper and stored on assets such as portable electronic storage devices; laptops, CD/DVDs, hard drives, solid state drives, flash memory sticks, etc.). It covers transport and transmittal between or within Restricted Access Areas (RAAs) of GC facilities (Canadian Embassies, military bases, missions or deployments and department/agency buildings) inside and outside Canada. This guide covers both small shipments such as letters and parcels that can be hand carried; and large or bulk shipments that due to size, weight, or nature cannot be hand carried and should be commercially transmitted (courier, mail service etc.). Portable electronic storage devices should only be used for the temporary transfer of information; they are not permanent storage devices.

It is impossible to address every situation in this guide. Employees should exercise good judgment and make every reasonable effort to minimize the risk to protected and classified material. Consult your Departmental Security Professionals for guidance.

1.3. Exclusions

Exclusions from this guide include:

- Electronic transmission of protected and classified material. Refer to Communication Security Establishment's (CSE) IT Security Directive for the Application of Communications

Security Using CSE-Approved Solutions (ITSD-01A), and IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network (ITSD-04A);

- The transport and transmittal of assets/equipment such as storage cabinets, computers, bulk equipment, etc. which do not contain protected and classified material (i.e. data wiped by CSE-approved methods or memory devices removed); consult departmental security procedures and ITSP 40.006 – IT Media Sanitization;
- The transport and transmittal of protected and classified material between the GC and industry. Ref: Public Service and Procurement Canada (PSPC) Contract Security Manual for specific safeguards while being transferred internationally;
- NATO Classified and NATO COMSEC material should be transmitted in Canada and to NATO nations in accordance with NATO and foreign national manuals. NATO Security Policy, C-M (2002)49 and supporting directives on security of information AC/35-D/2002; and
- Foreign COMSEC material should be transmitted in accordance with the CSEs IT Security Directive for the Control of COMSEC Material in the GC (ITSD-03A).

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, shipment tracking software or electronic inventory programs.

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 remain, and that any risks are 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
Alt	Alternate
CATSA	Canadian Air Transport Security Authority
CSP	Contract Security Program at PSPC
CSSS	Canadian SIGINT (Signals Intelligence) Security Standards
COMSEC	Communications Security
CONOPS	Concept of Operations
CSE	Communications Security Establishment
CSO	Chief Security Officer
DipMS	Diplomatic Mail Service
DMS	Departmental Messenger Service
GAC	Global Affairs Canada
GC	Government of Canada
HDD	Hard Disk Drive
IISD	International Industrial Security Sector
IT	Information Technology
LSA	Lead Security Agency
MOU	Memorandum of Understanding
PSPC	Public Service Procurement Canada
RAA	Restricted Access Area
RCMP	Royal Canadian Mounted Police
RCS	Reliable Courier Service
SA&A	Security Assessment and Authorization
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
USB	Universal Serial Bus

4. Glossary

Term	Definition
Appropriately Screened Service	A messenger or courier service working under contract with the GC where personnel are security screened to a level commensurate with the categorization level of the material they transmit.
Approved Dispatch Case	A briefcase approved by the RCMP for the transport of protected and classified material, and designed to provide adequate resistance against surreptitious attacks.
Bearer	A person or company moving protected or classified material between the originator and the recipient.
Bulk Shipment	Shipments that due to size, weight, or nature cannot be carried.
Carry Case	Includes any commercial off-the-shelf, hard or soft bag, backpack, briefcase (lockable or not) or RCMP approved dispatch case.

COMSEC Material	Material designed to secure or authenticate telecommunications. COMSEC material includes but is not limited to keys, equipment, devices, documents, firmware or software that embodies or describes cryptographic logic and other items performing COMSEC functions.
Departmental Messenger Service (DMS)	Any appropriately cleared employee or contractor working for the department to transmit protected and classified material.
Diplomatic Mail Service (DipMS)	A service provided by Global Affairs Canada (GAC) to provide secure delivery of unclassified, protected and classified material to and from missions outside Canada via diplomatic bag.
Electronic Storage Media	Any computing hardware used for storing, porting and extracting data files and objects. Includes CDs, DVDs, hard disk drives (HDDs) (removable and fixed), solid state drives (SSDs), USB keys, magnetic tapes and cartridges, secure digital (SD) and secure digital high capacity (SDHC) storage cards, and devices with internal storage such as computers, laptops, cell phones, and tablets.
Electronic Transmission	The transfer of protected and classified material using an approved electronic communications method or system.
Envelope	A commercial-grade, sealable, paper stock or polyethylene, opaque envelope with no windows, jacket, opaque wrapper or cover used to safeguard protected and classified material.
Letter Mail	Standard: Maximum dimensions of 245 mm x 156 mm weighing 50 g or less. Non-standard: Maximum dimensions of 380 mm x 270 mm weighing 500 g or less. Parcel: Any package exceeding the dimensions or weight of non-standard letter mail.
Nested Envelopes	Packaging of protected or classified material in two sealed layers. An inner layer with addresses and categorization level. An outer layer with addresses, but no categorization indication.
Originator	The person sending the protected or classified material.
Outside Canada	Areas not within the borders of Canada including GC facilities (i.e. embassies, missions or deployments, department buildings, consulates) in foreign countries.
Recipient	The person receiving the protected or classified material.
Registered Mail	A postal mailing term/service for letter-mail only. Provided by Canada Post or equivalent service abroad, which provides the sender with proof of mailing and/or proof of delivery in the form of receipts and signatures and dates.
Reliable Courier Service	A security-screened commercial company endorsed to deliver protected and classified material within Canada.
Restricted Access Area (RAA)	A work area (site or building) within a department where access is limited to authorized individuals. This includes Operations Zone, Security Zone, and High Security Zones as defined in Ref: G1-026 Guide to the Application of Physical Security Zones.

Security Categorization	The process of assigning a security category to information resources, assets or services based on the degree of injury that could reasonably be expected to result from their compromise.
Security Container	Security containers include any RCMP approved security cabinets, cases, or boxes, included in G1-001 Security Equipment Guide. It may also include a Secure Storage Room if built to the specifications outlined in G13-01 – Secure Storage Room Guide
Security Markings	Information or asset markings to indicate the security categorization of the material.
Surreptitious Attack	A secret, unauthorized attack to breach or circumvent a defensive system or some of its components in such a manner that the custodians and/or security force cannot readily detect the attack.
Transmittal	Send (e.g. courier/mail) protected or classified material from originator to recipient by a third party. The bearer may not have the need-to-know.
Transport	Carry protected or classified material to the recipient. The bearer is either the originator or the recipient and should have need-to-know.
Unauthorized Disclosure	An event involving the exposure or disclosure of material to individuals not authorized to access the material.

5. Transport and Transmittal

5.1. General Guidelines / Safeguards

Where feasible, protected and classified material should be sent by an approved electronic transmission method rather than physical transport or transmittal of hardcopy information or electronic storage media. Departments should consult the Directive on Security Management (DSM), CSEs IT Security Directive for the Application of Communications Security Using CSE-Approved Solutions (ITSD-01A), and IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network (ITSD-04A) for guidance.

Departments should transport or transmit protected or classified material at a level equal to or greater than the minimum or recommended requirements set out in this guide. Refer to charts 5.2 through 5.5 for summarized requirements. All electronic storage media containing protected or classified material to be transported or transmitted between GC facilities or zones should be encrypted using CSE-approved encryption. This protects against unauthorized disclosure due to accidental loss and surreptitious duplication.

When protected and classified material is transported or transmitted to, from or within foreign countries (particularly in non-NATO countries), there is a much higher risk of that material being compromised. GAC Diplomatic Mail Services (DipMS) is recommended for all categories of protected and classified material in these circumstances. Only a GAC Diplomatic courier (or a NATO accredited courier under specific circumstances) has diplomatic status and protection.

Anyone else will be subject to search and seizure. Contact GAC (DipMS) for detailed information.

Industrial security memoranda of understanding or arrangements with foreign nations may stipulate different standards for the transport and transmittal of protected and classified material between foreign and Canadian industries involved in protected and classified contracts and projects.

The responsibility to review and approve any transport or transmittal of Protected C, Secret or Top Secret material rests with the CSO however this may be delegated to departmental security professionals where necessary.

The security measures for transporting and transmitting protected and classified material largely depend on proper packaging, addressing and delivery, as well as anonymity and control of access to the material at all times.

When transporting or transmitting protected and classified material, a copy of the original should be transported or transmitted, and the original retained in the workplace; if not possible, the sender should keep a copy of the original at the workplace.

Communications Security Establishment (CSE) is responsible for defining the security infrastructure and procedures for protecting Signals Intelligence (SIGINT) produced or received by the Government of Canada. The CSE's Canadian SIGINT Security Standards (CSSS) are issued in accordance with CSE's role as national authority for SIGINT as established by section 5.46 of the Treasury Board of Canada Secretariat's (TBS), 2019 update to the Policy on Government Security (Policy on Government Security- Canada.ca). The CSSS-100, SIGINT Protection and Control, and its companion volumes are issued under the authority of the Chief of the CSE and are the authoritative Canadian SIGINT security standards. The CSSS policy suite is applicable to Canadian federal institutions and individuals authorized to access SIGINT information and assets, and are to be followed for the protection and handling of SIGINT. CSSS documents are available at CSE's Canadian Top Secret Network (CTSN) site, or by contacting CSE's SIGINT Security Management Office (SSMO).

5.1.1. Transport and Transmittal Basics

- Transport or Transmittal **Within Canada** means the originator, bearer, and recipient are and remain inside Canada during the transport or transmittal; and
- Transport or Transmittal **outside Canada** means either the originator, bearer, or recipient are (or are travelling) outside of Canada including within GC facilities (i.e. embassies, missions or deployments, department buildings, consulates) in foreign countries during the transport or transmittal.

5.1.2. Transport / Transmittal Routes

- **Within Restricted Access Areas (RAAs)** means the bearer remains inside a contiguous operations and higher security zone; and
- **Between RAAs** means the bearer passes through a reception or lower security zone.

5.1.3. Bearers

- The **Transport Bearer** is either the originator or the recipient; and
- The **Transport Alternate** is a list of alternate bearers in preferential order if the approved bearer is unavailable or unable to transmit the material.

5.2. Transport Guidelines for Protected Material

	Source / Destination	Preparation					Transport
		Receipt and Notify	Envelopes / Package	Address	Security Marking	Security Tape	Carry Case
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.6.4
Protected A	Within RAA in Canada	No	Cover/File folder	No	None	No	None
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack
	Within RAA outside Canada	No	Cover/File folder	No	None	No	None
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack - lockable
	RAA / Telework Remote in Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack
Protected B	Within RAA in Canada	No	Cover/File folder	No	None	No	None
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack
	Within RAA outside Canada	No	Cover/File folder	No	None	No	None
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack - lockable
	RAA / Telework Remote in Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack
Protected C	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	None
	Between RAAs in Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Commercial case / pack - lockable
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	None
	Either/both RAAs outside Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Approved Dispatch Case
	RAA / Telework Remote in Canada	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**

(1) Reference 5.6.4

5.3. Transmittal Guidelines for Protected Material

	Source / Destination	Preparation					Delivery Methods				
		Receipt and Notify	Envelopes / Package	Address	Security Marking	Security Tape	DMS	Canada Post	Reliable Courier	Registered Mail	DipMS
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.9.2	5.9.3	5.9.4	5.9.5	5.9.6
Protected A	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	1st alt.	N/A	2nd alt.	3rd alt.	**Yes**
Protected B	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	1st alt.	N/A	2nd alt.	3rd alt.	**Yes**
Protected C	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	Yes	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**Yes**	N/A	N/A	N/A	N/A
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**

(1) CSO approval required

5.4. Transport Guidelines for Classified Material

	Source / Destination	Preparation					Transport
		Receipt and Notify	Envelopes / Package	Address	Security Marking	Security Tape	Carry Case
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.6.4
Confidential	Within RAA in Canada	No	Cover/File folder	No	None	No	None
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	Commercial case / pack - lockable
	Within RAA outside Canada	No	Cover/File folder	No	None	No	None
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	Approved Dispatch Case
	RAA / Telework Remote in Canada	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**
Secret	Within RAA in Canada	No	**Sealed envelope** (Cover/File folder minimum)	No	None	No	None
	Between RAAs in Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Approved Dispatch Case or Commercial case / pack – lockable if CSO approved
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	None
	Either/both RAAs outside Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Approved Dispatch Case
	RAA / Telework Remote in Canada	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**
Top Secret	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	None
	Between RAAs in Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Approved Dispatch Case (Commercial case / pack – lockable if CSO approved)
	Within RAA outside Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	None
	Either/both RAAs outside Canada	No	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	Approved Dispatch Case
	RAA / Telework Remote in Canada	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**	**(1)**

(1) Reference 5.6.4

5.5. Transmittal Guidelines for Classified Material

	Source / Destination	Preparation					Delivery Methods				
		Receipt and Notify	Envelopes / Package	Address	Security Marking	Security Tape	DMS	Canada Post	Reliable Courier	Registered Mail	DipMS
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.9.2	5.9.3	5.9.4	5.9.5	5.9.6
Confidential	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Within RAA outside Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed envelope**	**Yes**	None	No	1st alt.	N/A	2nd alt.	3rd alt.	**Yes**
Secret	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Within RAA outside Canada	**Yes, Both**	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**
Top Secret	Within RAA in Canada	No	**Sealed envelope**	**Yes**	None	No	**Yes**	N/A	N/A	N/A	N/A
	Between RAAs in Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**Yes**	N/A	N/A	N/A	N/A
	Within RAA outside Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	**Yes, both**	**Nested envelopes**	**Yes, both envelopes**	**Yes, inner envelope**	**Yes, inner envelope**	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**

(1) CSO approval required

5.6. Preparation, Packaging and Addressing

Prior to transport or transmittal of protected and classified material, the sender, departmental security professional or delegated official should inventory the material. The sender should retain the original and send the copy; if not possible nor practicable, the sender should at least retain a copy before transporting or transmitting protected and classified material.

The packaging and carrying case used for transport and transmittal of protected and classified material should be durable enough to protect the material from damage and accidental exposure, and make it easy to detect evidence of tampering.

The packaging should be of a size and weight that allows the bearer to carry and retain in their personal possession. For oversize packages, refer to section 5.10 Bulk Shipments.

Fragile or irregular assets such as electronic storage media may require a padded or second envelope to allow for better protection of the contents.

The following preparation, packaging and addressing requirements apply to letters, envelopes, files, parcels, and drawing tubes.

5.6.1. Re-usable Cover/File Folder

This preparation method is only usable for Transport. The cover/file folder should:

- Hide the contents; and
- Have no security markings on the cover/file folder.

5.6.2. Single/Outer Envelope/Layer

Canvas bags, knapsacks, briefcases or other containers should not be used to replace the outer envelope or layer. A polyethylene single, outer envelope layer is preferred for transmittal as it resists accidental tearing while being handled.

The purposes for sealing the envelopes/layers are to prevent accidental exposure of the contents and to provide an indication of any tampering. Do not reuse previously sealed envelopes for protected or classified transport or transmittal as the initial use and opening will be indistinguishable from tampering and resealing.

Prior to sending, confirm the recipient's address as there may be different addresses for mailing and shipping. The single or outer envelope/layer of nested envelopes/layers should:

- Be sealed with integral adhesive or packing tape;
- Have no security markings on the envelope/outer layer;
- If transmittal by DipMS, show the address as Manager of Diplomatic Mail Services, GAC;
- For transmittal show the shipment or courier information;
- If a multi-part shipment (more than 1 package), show the package sequence number (ie. 2 of 3);

- Show the full return address of the sender;
- Show the full recipient address – non-specific when possible e.g. departmental mail room, or to a branch or section;
- When warranted by the "need-to-know" principle, single envelopes should have one of the following restrictive caveats:
  - When only a **position's incumbent** is to access the contents, show "**TO BE OPENED ONLY BY <position title>**"; and
  - When only the **identified individual** is to access the contents (usually personal information), show "**TO BE OPENED ONLY BY <name>**".

5.6.3. Nested Inner Envelope/Layer

The inner envelope/layer of nested envelopes/layers should:

- Be sealed with security tape on all seams;
- If applicable, contain Transmittal Note and Receipt form;
- Include an inventory of the contents;
- Have security markings of the highest categorization of the contents on two sides. This includes any special markings such as "Restricted NATO" or "NATO", or any special instructions;
- If a multi-part package, show the package sequence number (ie. 2 of 3) matching the sequence numbers on the outer envelope layer;
- Show the full return address of the sender;
- Show the full recipient address and attention line with a person's name and contact number;
- When warranted by the "need-to-know" principle, single or inner envelopes should be marked with one of the following restrictive caveats;
  - When only a **position's incumbent** is to access the contents, show "**TO BE OPENED ONLY BY <position title>**" on **both sides**; and
  - When only the **identified individual** is to access the contents (usually personal information), show "**TO BE OPENED ONLY BY <name>**" on **both sides**.

5.6.4. Transport Carrying Case for Protected and Classified Material

A carrying case (ie. canvas bags, knapsacks, brief cases, dispatch case or other container) when used for transporting sensitive material should be used in conjunction with the required packaging and should not be used to replace the outer envelope or layer.

It is not recommended that hardcopy or electronic Protected C, Confidential, Secret and Top Secret material be transported to, processed or stored in a Remote/Telework location. In situations where this is unavoidable, CSOs should review each request and only approve after a threat and risk assessment and Remote/Telework site inspection has been completed. This will help to ensure that all physical and IT security measures can be successfully implemented. The risk management decision to allow Protected C, Secret and Top Secret material in a Remote/Telework location rests with the department.

5.6.5. Transmittal Note and Receipt Form

It is recommended that a Transmittal Note and Receipt Form be included inside a single or inner envelope for all protected and classified material before transmitting. The Transmittal Note and Receipt Form is only used in the situations covered in the preceding transport and transmittal tables. A standard Transmittal Note and Receipt Form (GC-44) is available on the PSPC Website at gc44.xft (pwgsc.gc.ca) or departments may create their own using the following format and usage procedures.

- The form should indicate the point of origin, the name of the initiating branch or office, the date of dispatch, the security categorization level of the transmitted material and any unclassified detailed description of the contents of the shipment/package;
- Forms should be individually numbered, to facilitate the audit function, and comprise three copies, preferably color-coded. The original and a duplicate copy should be forwarded to the recipient - inside the same nested envelope as the material (where feasible). The triplicate should be retained on file until the receipted original is returned;
- The form should request a signature from the recipient and the date of reception, and require the return of the original copy by a prescribed time;
- If the signed original is not returned within the prescribed time, the sender should confirm receipt of the shipment from the recipient. If the recipient did not receive the shipment, call the transmittal delivery service to validate tracking before notifying the department unit security office or CSO of the incident; and
- When the material has been delivered at the destination, a receipt should be obtained from an appropriate official at the destination and the receipt returned to the appropriate official at the sending department.

5.7. During Transport

5.7.1. General

Prior to or while being transported, the following security measures should be adhered to for all protected and classified material:

- Prior to shipment, protected and classified material should be inventoried, a copy of the inventory retained and another copy placed inside the package;
- Stay in the personal possession of the bearer at all times, except when placed in authorized storage (Ref. 5.7.5);
- Not to be opened enroute except, if required, at border crossing and airport checkpoints (Ref., 5.7.3, 5.7.4);
- Protected or classified material should not be read, displayed or processed in public (for example, on a bus, train, airplane, coffee shop, library etc.); and
- Upon return, the traveler should return all protected and classified material in a sealed package, or produce a receipt signed by a departmental security representative of the addressee organization, for any material that is not returned.

5.7.2. Transport by Vehicle

While traveling by vehicle, the bearer should place protected and classified material in a carrying case or dispatch case and lock it in the trunk or out of sight in a locked vehicle.

The case is to be placed in the trunk at the time of departure and remain there until taken out at destination point or at a stopover. The material must never be left in an unattended vehicle.

Note: This applies to a personal motor vehicle and not vehicles that carry public passengers. Public transportation procedures require that the case remain in the person's possession or control.

5.7.3. Transport by Air

If Protected C, Secret, or Top Secret material is being carried by the transport bearer on a commercial air flight starting in Canada, it is recommended to make advance arrangements with the CATSA regional manager (at departing airport). CATSA is responsible for pre-board screening at all designated Canadian airports. At the pre-board screening checkpoint, the bearer will present their identification and a certificate signed by a departmental or agency official attesting to the nature of the document or item. The certificate information should correspond with the identification information. Without proper documentation, the item will be subject to normal screening procedures.

5.7.4. Transport over Border Crossings and Airport Checkpoints

Apart from NATO and GAC Diplomatic couriers, there is no assurance of immunity from search by customs, police and/or immigration officials of the various countries whose border the bearer may cross. Therefore, contact your CSO for departmental policy and procedures when crossing borders and airport security checkpoints.

The bearer should proceed through the airline ticketing and boarding procedure as for other passengers. The bearer should not let carry-on luggage be inspected without their supervision and not out of their sight. Requests for customs or security inspection should not be denied. Care should be taken however to limit disclosing the protected and classified material – as to satisfy the official. If a shipment containing the protected and classified material is required to be opened, it should be done in an area out of sight of the public, if possible. The bearer must notify their CSO at the earliest possible time of any compromised material.

5.7.5. Transport with Overnight Stopovers

Protected C, Secret and Top Secret material shall not be left unattended under any circumstances. During overnight stops, Protected C, Secret and Top Secret material should be stored at Canadian military facilities, Canadian Embassies, other GC facilities, or appropriately security cleared contractor facilities. Material should never be stored in vehicles, traveler convenience lockers (usually found in bus terminals and train stations), hotel rooms or safes, personal residences, or any other unauthorized storage facility or location.

All other categorizations of protected and classified material should remain in the possession of the person transporting. Where this is not possible, secure dispatch cases

or lockable bags out of sight, preferably in a hotel safe. Photograph the location and packaging for comparison upon return and verification of signs of tampering.

Bearers are to make every reasonable effort to plan their itinerary to ensure that stopovers are eliminated before reaching a final destination. However, if brief unforeseen or planned stopovers are necessary (i.e. meal breaks, etc.), the bearer should exercise good judgment and ensure that every reasonable effort is made to minimize the risk to the protected and classified material.

5.8. Delivery

The recipient of protected and classified material transported or transmitted should:

- Ensure that the packaging is intact and has not been tampered with;
- If a multi-part package, confirm all parts are received;
- Verify the contents against the included inventory; and
- Report any discrepancies, damage, or evidence of tampering to the CSO.

5.9. Transmittal Methods

5.9.1. General

Protected and classified material is considered "in transmittal" until it has reached its intended destination and has been delivered to the addressee. Once opened, it should be safeguarded in accordance with Section 7 – Storage.

It is recommended that a Transmittal Note and Receipt Form be included inside the inner envelope for all protected and classified material before transmitting. Refer to section 5.6.5 Transmittal Note and Receipt Form .

The departmental CSO should review and approve any request or requirement to transport or transmit Protected C, Secret or Top Secret material outside of Canada that is not sent by GAC DipMS, IIDS or NATO Couriers via DND.

5.9.2. Departmental Messenger Service (DMS)

When protected and classified material is transmitted via Departmental Messenger Service, the delivery personnel should ensure that a specific departmental mailroom, section or the intended recipient receives the mail.

Some departmental mailroom employees who are not cleared to a level commensurate with the material they control may open mail before it reaches its intended recipient. Departments should complete a TRA to determine the safeguards required for enhanced mailroom security, including handling and opening mail.

Mail marked "to be opened only by the addressee" should be delivered to the intended recipient directly and under no circumstances should this mail be opened by anyone else except the intended recipient.

5.9.3. Canada Post

If using Canada Post for transmittal between RAAs within Canada, the material should be sent by first class mail or parcel post.

Canada Post relies on agreements with the postal services of foreign countries and the Universal Postal Union. International mail (letter-post) delivered by Canada Post is dropped off at Customs before it is passed on to the foreign postal service. There is no guarantee of proof of delivery since this service varies from country to country. Prior to sending any protected and classified material outside Canada via Canada Post, the postal service agreement with the other country should be checked on the Canada Post web site (www.canadapost.ca) or by contacting Canada Post directly. If regular post must still be used, include a Transmittal Note and Receipt Form with the shipment as per ref 5.6.5.

5.9.4. Reliable Courier Service

The transfer of protected and classified material between Canadian and foreign governments and industry, as a result of protected and classified contracts, should be arranged by the International Industrial Security Directorate (IISD-PSPC) through government-to-government channels. Strict procedures should be followed to ensure proper handling and safeguarding of such material while in-transit, both nationally and internationally.

When appropriately screened courier services are required, contact IISD for advice. Departments wishing to have a courier company security cleared for the transport and transmittal of protected and classified material within Canada may sponsor the company and have them added to a list of appropriately cleared companies. All appropriately screened courier services should be able to supply a record of mailing, routing, and delivery.

CSP will only clear companies that have active contracts procured through PSPC. If departments want to have a courier company cleared, there needs to be a contract submitted to the CSP identifying the level of clearance required.

5.9.5. Registered Mail

Registered mail is an alternative for use when one or both the source and destination RAAs are outside Canada. A receipt signature and letter/parcel tracking are required. Using this service requires CSO approval and should only be used as a last resort for Protected C, Secret, and Top Secret transmittal. Departmental Messenger Service or a reliable courier are preferred alternatives.

5.9.6. Diplomatic Mail Service (DipMS)

The DipMS of GAC provides all diplomatic courier services inside and outside Canada. Any exception to the use of DipMS requires the CSO's approval.

5.10. Bulk Shipments

Bulk shipments are transmittal only, and occur between RAAs in, or outside Canada. A delivery service should be selected that will provide direct service from point of origin to point of destination. When such a service is not available, arrangements should be made for overnight storage. (Refer to section 7.2 Storage During Transmittal)

Guidelines for bulk transmittals are:

- The transmittal should be handled with the requirements for the highest categorization;
- Protected and classified material bulk shipments should be placed in an inner enclosure (wrapped or boxed in paper, wood or a combination thereof), tape-sealed and tagged/labelled with package number;
- Protected C, Secret and Top Secret inner enclosures should be placed in a secure outer enclosure (crate, transit case, etc.), sealed (taped or metal strapping) and / or padlocked (heavy duty reinforced shackle with high security keyway);
- When transmitting large quantities of Protected C, secret and Top Secret material by bulk shipment is required, consider transmitting in separate, smaller packages. A focused TRA may indicate additional safeguards to use to protect this quantity of material;
- If there are multiple packages, mark on the outer enclosure of each package the package number as well as the total number of packages (ie. 1/3, 2/3 3/3);
- The enclosures for bulk shipments of protected and classified material should be addressed as per sections 5.6.2 and 5.6.3;
- When traveling by air, bus, truck or train, the outer enclosure should be checked in as cargo baggage. The shipment may require escort by appropriately screened personnel when warranted by a TRA. In such cases, advance arrangements with carriers are required. Escorts should provide continuous observation of the shipment during stops or layovers;
- For bulk transmittal using containers, rail cars, or trucks, the container, rail car, or truck should have all doors sealed and padlocked using a heavy-duty, reinforced shackle lock with a high security keyway. The seals and locks should be applied and verified for integrity before removal by appropriately screened personnel and be verified against the manifest with copies retained by both the originator and the recipient. The shipment may be required to be escorted by appropriately-screened personnel when warranted by a TRA;
- Protected A, B and Confidential security level shipments inside Canada should have a TRA completed prior to the shipment;
- Protected C, Secret, and Top Secret security level shipments inside Canada should:
  - Have a TRA completed prior to the shipment;
  - Be reviewed and approval by the CSO;
  - Have an appropriately screened escort;
- It is strongly recommended that bulk shipments of all protected and classified material transmitted outside Canada be handled by GAC DipMS;
- If GAC DipMS is not doing the bulk the shipment of protected and classified material outside of Canada, a TRA should be completed and the shipment approved by the CSO (or delegate). The bulk shipment should be escorted by appropriately screened providers;
- Protected C, Secret, and Top Secret security level shipments outside Canada should:
  - Be sent by DipMS outside of Canada; and
- TRAs for bulk shipments should account for the type of carrier that is being used.

5.11. Bulk Transmittal Guidelines for Protected Material

	Source / Destination	Preparation					Delivery Methods				
		Receipt and Notify	Package	Address	Security Marking	Security Tape	DMS	Canada Post	Reliable Courier	Registered Mail	DipMS
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.9.2	5.9.3	5.9.4	5.9.5	5.9.6
Protected A (3)	Between RAAs in Canada	No	**Sealed package**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed package**	**Yes**	None	No	1st alt.	N/A	2nd alt.	3rd alt.	**Yes**
Protected B (3)	Between RAAs in Canada	No	**Sealed package**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed package**	**Yes**	None	No	1st alt.	N/A	2nd alt.	3rd alt.	**Yes**
Protected C (2)	**(4)** Between RAAs in Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	**Yes, inner layer**	**Yes**	N/A	N/A	N/A	N/A
	(4) Either/both RAAs outside Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	**Yes, inner layer**	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**

(1) CSO approval required
(2) TRA required
(3) TRA optional
(4) Appropriately screened escort required

5.12. Bulk Transmittal Guidelines for Classified Material

	Source / Destination	Preparation					Delivery Methods				
		Receipt and Notify	**Package**	**Address**	**Security Marking**	**Security Tape**	**DMS**	**Canada Post**	**Reliable Courier**	**Registered Mail**	**DipMS**
Ref	5.1	5.6.5	5.6	5.6	5.6	5.6.3	5.9.2	5.9.3	5.9.4	5.9.5	5.9.6
Confidential (3)	Between RAAs in Canada	No	**Sealed package**	**Yes**	None	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Either/both RAAs outside Canada	No	**Sealed package**	**Yes**	None	No	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**
Secret (2)	**(4)** Between RAAs in Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	No	**Yes**	1st alt.	2nd alt.	N/A	N/A
	Either/both RAAs outside Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	No	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**
Top Secret (2)	**(4)** Between RAAs in Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	**Yes, inner layer**	**Yes**	N/A	N/A	N/A	N/A
	Either/both RAAs outside Canada	**Yes, both**	**Two-layer package**	**Yes, both layers**	**Yes, inner layer**	**Yes, inner layer**	**(1)** 1st alt.	N/A	**(1)** 2nd alt.	**(1)** 3rd alt.	**Yes**

(1) CSO approval required
(2) TRA required
(3) TRA optional
(4) Appropriately screened escort required

5.13. Special Considerations

5.13.1. NATO Classified and NATO & Foreign COMSEC Material

- NATO Classified and NATO COMSEC material should be transmitted within Canada and to NATO member nations in accordance with NATO and foreign national manuals. Refer to the NATO Security Policy, C-M (2002)49 and supporting directives on security of information AC/35-D/2002; and
- Foreign COMSEC material should be transmitted in accordance with the CSEs IT Security Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A).

5.13.2. Mailrooms

- Departmental mailroom employees who are not cleared to a level commensurate with the material they control may be required to open mail before it reaches its intended recipient. Departments should complete a TRA to determine the safeguards required for enhanced mailroom security, including and opening mail; and
- Mail marked "to be opened only by the addressee" should be delivered to the intended recipient directly and under no circumstances should this mail be opened by anyone else except the intended recipient.

5.13.3. Portable Electronic Data Storage Devices

- Portable Electronic Devices - This category of devices includes laptops, diskettes, CD/DVDs, hard drives (both removable and permanent), flash memory sticks, USB hard drive or keychain drives, mobile phones, smart watches, digital cameras with smart media cards, storage cartridges, video displays, magnetic tapes and cassettes, and other similar devices that may contain protected and classified material in electronic form;
- TRA Requirements - A department-specific TRA should be conducted to determine what safeguards may be required to transport or transmit Protected B, Protected C and all classified material on electronic storage devices (including USBs, CD/DVDs, and external/removable hard drives);
- Transport and Transmittal - Portable devices that contain protected and classified material should be transported, transmitted and stored in the same manner as paper material. This should be commensurate with the categorization level of the material they contain or process and the assessed level of risk. This means that if these devices are not encrypted in accordance with the existing GC Information Technology Security Standards, they should, as a minimum, be placed in an envelope, carrying case or approved dispatch case as per section 5. Additional safeguards may be required in this case based upon any TRA recommendations. If the device is password-controlled and has CSE-approved encryption, it does not have to be placed in an envelope or carrying case but it should be kept under the constant control/possession of the bearer at all times, such as in the bearer's pocket or purse, etc. The CSO should approve any transport or transmittal of Protected C, Secret or Top Secret material if not sent by GAC DipMS, IISD or NATO couriers via DND;

- Removal from Workplace - Portable electronic data storage devices containing protected and classified material may be authorized for removal from the departmental workplace - however, they are susceptible to theft or loss. Therefore, when not in use they should be protected in accordance with departmental security policies (ie. authorization of CSO or other CSO-authorized responsible manager, and recorded). The security policy could include security measures such as password controls and CSE approved encryption of Protected B (when warranted by the TRA), Protected C, and all classified material. Before transport or transmittal, protected and classified material contained on the devices should be backed up if not recorded elsewhere;
- Laptops - Laptops containing protected and classified material with no CSE-approved encryption protection should be carried in a locked carrying case of such size and weight that it can be retained in the personal possession of the individual at all times. In Canada, laptops with password controls and CSE-approved encryption do not require being in a locked carrying case or approved dispatch case. Consideration should however, be given based upon specific security concerns or threats. Outside Canada, however, a locked carrying case should be used. When warranted by a TRA for detection of tampering, an approved tamper-indicating security polyethylene envelope may be used. When traveling by personal vehicle, the laptop should be locked in the trunk out of plain sight and never left unattended;
- In Transit - Portable electronic storage devices with protected and classified material must be kept under the possession and constant control of the bearer at all times. The material stored on these devices should not be viewed in public places (e.g. buses, trains, airports, restaurants, coffee shops); and
- Overnight Stopovers - During overnight stopovers portable electronic storage devices should be treated in the same manner as paper material (refer to section 5.7.5).

5.14. Lost or Missing Shipments

Shipments that are lost or fail to reach the destination within the expected delivery time must be reported to the CSOs and departmental security groups of both the originating and receiving departments. An investigation must be launched to determine what happened; where the shipment is and the probability and degree of compromise. Steps must be taken to recover the material and address any security concerns that may have, or will occur due to the loss of the material.

6. Enhanced Safeguards

Enhanced security safeguards for the transport and transmittal of protected and classified material may be appropriate depending on the recommendations of the TRA. Consider transporting or transmitting lower categories of protected or classified material as per the next higher category level (ie. forward Protected A using the requirements for Protected B, Confidential using the requirements for Secret).

For material with a significant risk associated with it, consider additional safeguards including:

- Transport and Transmittal:
  - Use a Nested Envelope for the material;
  - Security marking the inner envelope;
  - Security taping the inner envelope;
  - A polyethylene inner envelope / layer may be required for improved tamper detection when a TRA indicates enhanced security measures are required; and
  - Use of a lockable carry case or approved dispatch case.

- Transmittal:
  - GAC DipMS; and
  - Initiate Transmittal Note and Receipt Form.

7. Storage

7.1. Storage General

Protected and classified material must be stored in approved containers and appropriate zone as per the minimum requirements laid out in the charts in section 7.10 and 7.11.

Protected and classified research and development equipment, engineering models or prototypes must be stored in containers approved for that purpose or as listed in the RCMP Security Equipment Guide. For requirements not met by items listed in the Security Equipment Guide, contact the RCMP LSA (RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca).

Care needs to be taken to ensure that classified and protected material including valuable material are properly safeguarded when occupants are away from their workstations for any length of time. This includes Remote and Telework environments or when working in places other than the designated GC work site.

7.2. Security Containers

Security containers include any RCMP approved security cabinets, cases, boxes, or bags included in G1-001 Security Equipment Guide. Security containers may also include a Secure Storage Room if built to the specifications outlined in G13-01 – Secure Storage Room Guide.

When different levels of protected or classified material is stored together, storage should comply with the standard set for the highest categorization of material involved. The infrequent storage of a relatively small amount of material having high-level categorization with a larger amount of material with a low-level categorization may not necessarily warrant enhanced safeguards, however this must be risk managed by the department.

Protected and classified material should not be stored with valuables such as cash or other monetary instruments or drugs in the same security container.

Approved dispatch cases or other lockable carry cases must not be used as permanent storage

containers and should not be used as such.

Departments must develop procedures for the storage of assets shared with the GC, other Canadian governments, foreign governments, international, educational and private sector organizations. Procedures must be in accordance with agreements or arrangements between the parties concerned and all relevant policies and guidelines.

All employees working in locations other than a GC designated work site (ie. Remote or Telework environments) must safeguard material as per the minimum requirements outlined in GCPSG-008 - Physical Security Considerations for Remote and Telework Environments. Employees should also consult the TBS Policies and their own departmental standards on Remote and Telework. With respect to off-site contract work, departments should consult with PSPC CSP and use the Security Requirements Checklist (TBS/SCT 350-103) PART A- CONTRACT INFORMATION / (canada.ca) to define the contract requirements for safeguarding protected or classified material at the contractor's facilities.

7.3. Storage of Valuable Assets

Valuable assets must be afforded protection against loss, destruction or alteration. The degree of protection afforded is dependent on the asset itself and the TRA. Some protection measures are contained in the RCMP Guide G1-001 - Security Equipment Guide. For additional information, contact the RCMP LSA.

7.4. Keys for Security Containers

Keys in this section include mechanical keys, combinations, personal identification numbers, and access cards. Keys for security containers must be safeguarded commensurate with the highest categorization level of the material to which the key provides access. This requirement also applies to records that would allow the reproduction of a key.

Keys that provide access to security containers should be changed annually and must be changed when:

- There is evidence of compromise;
- A TRA assessment indicates an unacceptable level of risk; or
- An employee's need to access the security container has changed.

A record of all changes to keys for security containers must be kept, including: the date, reason, custodian, location and, if applicable, lock identifier, combination number, duplicates, etc. This record of change must be secured commensurate with the highest security categorization of the material being protected within the container.

7.5. Disposal or Recycling of Security Containers

Departments are responsible for the disposal of security containers. Approved high security containers must not be disposed of or resold to private sector or outside agencies. Refer to RCMP Guide G1-001 - Security Equipment Guide. Departments are responsible for ensuring that prior to disposal or recycling, all containers are stored in an operations zone as a minimum, all contents have been removed and record logs have been amended accordingly.

7.6. Service and Maintenance of Security Containers

Departments must ensure that approved security containers are properly serviced and maintained at all times. Refer to RCMP Guide G1-001 - Security Equipment Guide.

7.7. Storage During Transport

Protected C and all classified material are not – under any circumstances – to be left unattended. During overnight stops, Protected C, Secret and Top Secret material should be stored at Canadian military facilities, Canadian Embassies, other GC facilities, or cleared contractor facilities. It must never be stored in vehicles, traveler convenience lockers (usually found in bus terminals and train stations), hotel rooms or safes, personal residences, or any other unauthorized storage facility or location. A TRA may include this storage requirement for Protected B material.

7.8. Storage During Transmittal

The GAC DipMS is responsible for storing the material they move outside of Canada. Storage during transmittal within Canada is the responsibility of the messenger, courier or mail service.

7.9. Protected and Classified Storage Requirements

All protected and classified material should be protected from overview when in the presence of a person without a "need-to-know".

Except where specified by specific guidance documents with identified requirements, protected and classified material should only be accessed within the appropriate physical security zone. Protected A, B and Confidential material requires an Operations Zone as a minimum, Protected C, Secret, and Top Secret material requires a Security or High Security Zone as a minimum.

7.10. Minimum Storage Guidelines for Protected Material

	Location	Zone	Storage	
			Temporarily away	Not in Use
Protected A	Within RAA in Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
	Within RAA outside Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
Protected B	Within RAA in Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
	Within RAA outside Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
Protected C	Within RAA in Canada	Security	Locked in security container	Locked in security container
	Within RAA outside Canada	High Security	Locked in security container	Locked in security container

7.11. Minimum Storage Guidelines for Classified Material

	Location	Zone	Storage	
			Temporarily away	Not in Use
Confidential	Within RAA in Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
	Within RAA outside Canada	Operations	Covered or turned down or in closed drawer	Locked file cabinet or desk drawer
Secret	Within RAA in Canada	Security	Locked in security container	Locked in security container
	Within RAA outside Canada	Security	Locked in security container	Locked in security container
Top Secret	Within RAA in Canada	High Security	Locked in security container	Locked in security container
	Within RAA outside Canada	High Security	Locked in security container	Locked in security container

8. References and Related Documents

- Policy on Government Security – Policy on Government Security- Canada.ca
- Directive on Security Management – Directive on Security Management- Canada.ca;
- G1-026 Guide to the Application of Physical Security Zones – G1-026 Guide to the Application of Physical Security Zones - Royal Canadian Mounted Police (rcmp-grc.gc.ca)
- Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111) – Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111) - Canadian Centre for Cyber Security;
- IT Security Directive for the Application of Communications Security Using CSE-Approved Solutions (ITSD-01A) –IT Security Directive for the Application of Communications Security Using CSE-Approved Solutions (ITSD-01A) - Canadian Centre for Cyber Security;
- Sanitization and Disposal of Electronic Devices (ITSAP.40.006) – Sanitization and disposal of electronic devices (ITSAP.40.006) - Canadian Centre for Cyber Security
- IT Security Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) – IT Security Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) - Canadian Centre for Cyber Security;
- IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network (ITSD-04A) – IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network (ITSD-04A) - Canadian Centre for Cyber Security;
- Guidance for the Communications Security of SECRET Information (ITSB-79) – Guidance for the communications security of SECRET Information (ITSB-79) - Canadian Centre for Cyber Security;
- Canada Post – Mailing and shipping for Personal and Business | Canada Post (canadapost-postescanada.ca);
- Canadian Air Transport Security Authority (CATSA) –Welcome / Bienvenue | CATSA | ACSTA (catsa-acsta.gc.ca); and
- Global Affairs Canada – Diplomatic Mail Service and Mail Handling Procedures at Missions (contact 1-866-634-6245 or in Ottawa at 944MAIL (944-6245)).

9. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-007 (2022) – Transport, Transmittal and Storage of Protected and Classified Material, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2022.10.13 11:48:05 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-007 (2022) – Transport, Transmittal and Storage of Protected and Classified Material.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2022.10.21 10:00:15 -04'00'

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

Date