
ROYAL CANADIAN MOUNTED POLICE

SSB/SG - 30

**STANDARD FOR THE TRANSPORT AND TRANSMITTAL
OF SENSITIVE INFORMATION AND ASSETS**

June 1994

TABLE OF CONTENTS

PAGE

1	Introduction	<u>1</u>
1.1	Purpose and scope	<u>1</u>
1.3	Definitions	<u>1</u>
2	General Safeguards	<u>2</u>
2.1	In Canada - within a controlled area	<u>2</u>
2.2	In Canada - outside a controlled area	<u>2</u>
2.3	Outside Canada - within a controlled area	<u>4</u>
2.4	Outside Canada - outside a controlled area	<u>4</u>
3	Detailed Specifications	<u>5</u>
3.1	Enveloping	<u>5</u>
3.2	Addressing	<u>6</u>
3.3	Delivery responsibility	<u>6</u>
4	Sensitive Information and Assets at Higher Risk	<u>7</u>
4.1	General	<u>7</u>
4.2	Transport or transmittal outside Canada	<u>7</u>
4.3	Transport or transmittal to industries outside Canada	<u>8</u>
4.4	Additional safeguards	<u>8</u>
APPENDICES		
Chart A	Transport - in Canada	<u>9</u>
Chart B	Transport - outside Canada	<u>10</u>
Chart C	Transmittal - in Canada	<u>11</u>
Chart D	Transmittal - outside Canada	<u>12</u>

1 Introduction

1.1 Purpose and scope

This document is the standard for the transport and transmittal of sensitive information and assets as required by the security policy of the government of Canada (GSP). It contains both minimum requirements and recommended safeguards. Use of the word "must" in sentences in italics indicates a requirement. Use of the word "should" indicates safeguards to be applied unless a threat and risk assessment indicates otherwise.

While departmental or facility threat and risk assessments (TRAs) should address the transport and transmittal of sensitive information and assets specifically, the safeguards outlined in Sections 2 and 3 will satisfy the vast majority of these TRAs. Sensitive information and assets at higher risk, such as those described in Section 4, probably require more creative or additional safeguards.

1.2 Roles and responsibilities

Departments are responsible for the implementation of the standard. The RCMP is responsible for the development, approval and issuance of the standard and for advising on its application.

1.3 Definitions

Appropriately-screened personnel: for transmittal, this means persons screened, as required by the GSP, to a level commensurate with the information or assets they control.

Approved equivalent container: a container examined in accordance with the custom-test program and recommended by the test authority.

Classified information dispatch case: a specially-designed briefcase listed in the Security Equipment Guide (SSB/SG 20) for the purpose of carrying information designated extremely sensitive or classified secret or top secret.

Controlled area: an area comprised of any combination of the three restricted zones (defined later in this article).

Envelope: the jacket, wrapper or cover used to enclose sensitive information and assets.

Proprietary mail or messenger service: a service provided by: (a) personnel appointed by the departmental authority for the routine transmittal of sensitive information and assets, or (b) an individual endorsed on a case-by-case basis by a departmental employee for the transmittal of sensitive information and assets.

Restricted zone: any of three zones, the Operations Zone, the Security Zone or the High-Security Zone, to which access is restricted. (See 2.9 of the Physical Security Standard).

Sensitive asset: defined in the GSP as a classified or designated asset.

Sensitive information: defined in the GSP as classified or designated information.

Transmit: to transfer sensitive information and assets from one person or place to another by someone without a need-to-know the information or need-to-access the asset.

Transport: to transfer sensitive information and assets from one person or place to another by someone with a need-to-know the information or need-to-access the asset.

2 General Safeguards

Departments must transport or transmit sensitive information and assets according to the following minimum requirements.

2.1 In Canada - within a controlled area

(a) Transport

(i) Information and assets that are designated low sensitive or particularly sensitive or classified confidential or secret must be transported discreetly.

(ii) Information and assets that are designated extremely sensitive or classified top secret must be transported in a single envelope (may be reusable) with no security marking.

(b) Transmittal

(i) Information and assets that are designated low sensitive or particularly sensitive, or are classified confidential or secret must be transmitted via proprietary mail or messenger service, using a single envelope (may be reusable) with no security marking and addressed as in 3.2.

(ii) Information and assets that are designated extremely sensitive or classified top secret must be transmitted by a proprietary mail or messenger service, using a single, sealed envelope with no security marking and addressed as in 3.2. See also 3.1.

2.2 In Canada - outside a controlled area

(a) Transport

(i) Information and assets that are designated low sensitive or particularly sensitive must be transported in a single envelope (may be reusable) with no security marking and addressed as in 3.2. See also 3.1.

(ii) Information and assets that are classified confidential or secret must be transported in a single, sealed envelope with no security marking and addressed as in 3.2. See also 3.1.

(iii) Information and assets that are designated extremely sensitive or classified top secret must be transported in a single, sealed, security-marked envelope which is enclosed in a locked briefcase or other equally secure container. Address as in 3.2.

(b) Transmittal

(i) Information and assets that are designated low sensitive or particularly sensitive must be transmitted via:

- *a proprietary mail or messenger service. Enclose in a single envelope (may be reusable) with no security marking and address as in 3.2. See also 3.1; or*
- *first class mail. Enclose in a single, sealed envelope with no security marking and address as in 3.2. See also 3.1; or*
- *a reliable (see article 3.4) courier or similar postal service which provides proof of mailing and will supply, on request, a record of transit, and record of delivery. Envelope and address as for first class mail. This type of service should be used only when prompt delivery is essential.*

(ii) *Information and assets that are classified confidential or secret must be transmitted via:*

- *a proprietary mail or messenger service:*
 - *Enclose individual pieces of mail in a single, sealed envelope with no security marking and address as in 3.2. See also 3.1; or*
 - *When the option at 3.1.(a)(i) is used for bulk mail, locks or seals must be applied at the departure point and removed at the reception point (i.e. "**be controlled**") by appropriately-screened personnel. Address as in 3.2; or*
- *first class mail. Enclose in a single, sealed envelope with no security marking and address as in 3.2. See also 3.1; or*
- *a reliable (see article 3.4) courier or similar postal service which provides proof of mailing and will supply, on request, a record of transit, and record of delivery. Envelope and address as for first class mail. This type of service should be used only when prompt delivery is essential.*

(iii) *Information and assets that are designated extremely sensitive or classified top secret must be transmitted via:*

- *a proprietary mail or messenger service:*
 - *Enclose individual pieces of mail in a double envelope, security-mark the inner envelope only and address as in 3.2. See also 3.1(a)(i); or*
 - *When the option at 3.1(a)(i) is used for bulk mail, locks or seals must be applied at the departure point and removed at the reception point (i.e. "**be controlled**") by appropriately-screened personnel. Address as in 3.2; or*
- *registered mail. Double-envelope, security-mark the inner envelope only and address as in 3.2. See also 3.1(a); or*
- *a reliable (see article 3.4) courier or similar postal service which provides proof of mailing and will supply, on request, a record of transit, and record of delivery. Envelope and address as for registered mail. This type of service should be used only when prompt delivery is essential.*

2.3 Outside Canada - within a controlled area

(a) Transport

(i) Information and assets that are designated low sensitive or particularly sensitive must be transported discreetly. An envelope is not required.

(ii) Information and assets that are designated extremely sensitive or are classified confidential, secret or top secret must be transported in a single envelope (may be reusable) with no security marking and addressed as in 3.2. See also 3.1.

(b) Transmittal

(i) Information and assets that are designated low sensitive or particularly sensitive or classified confidential must be transmitted via proprietary mail or messenger service, using a single envelope (may be reusable) with no security marking and addressed as in 3.2. See also 3.1.

(ii) Information and assets that are designated extremely sensitive or classified secret or top secret must be transmitted by a proprietary mail or messenger service, using a single, sealed envelope with no security marking and addressed as in 3.2. See also 3.1.

2.4 Outside Canada - outside a controlled area (See also 4.2 and 4.3)

(a) Transport

(i) Information and assets that are designated low sensitive or particularly sensitive, or are classified confidential must be transported in a single, sealed envelope with no security marking and addressed as in 3.2. See also 3.1.

(ii) Information and assets that are designated extremely sensitive or classified secret or top secret must be transported in a double envelope. Security-mark the inner envelope only. Address as in 3.2. See also 3.1.(a)(ii).

(b) Transmittal

(i) Information and assets that are designated low sensitive or particularly sensitive must be enclosed in a single, sealed envelope with no security markings and addressed as in 3.2. See also 3.1. Transmit via:

- *a proprietary mail or messenger service; or*
- *first class mail (or equivalent service abroad); or*
- *a reliable (see article 3.4) courier service which provides proof of mailing and will supply, on request, a record of transit and record of delivery. This type of service should be used only when prompt delivery is essential.*

(ii) Information and assets that are classified confidential must be transmitted via:

- *a proprietary mail or messenger service:*

- *When transmitting individual pieces of mail by appropriately-screened personnel enclose in a single, sealed, envelope with no security marking. Address as in 3.2, see also 3.1; or*
- *When mail is not transmitted by appropriately-screened personnel or is in a bulk shipment, use option at 3.1(a)(i). Locks or seals must be applied at the departure point and removed at the reception point (i.e. "be controlled") by appropriately-screened personnel. Address as in 3.2; or*
- a reliable (see article 3.4) courier service which provides proof of mailing and will supply, on request, a record of transit and record of delivery. Enclose in a single, sealed envelope with no security marking and address as in 3.2. See also 3.1; or
- Department of Foreign Affairs and International Trade (DFAIT) Diplomatic Security Mail Service enclosed in a double envelope. Security-mark the inner envelope and address as in 3.2.

(iii) Information and assets that are designated extremely sensitive or classified secret or top secret must be transmitted via:

- a proprietary mail or messenger service:
 - when transmitting mail by appropriately-screened personnel use a double envelope and place a Sensitive Information and Assets Receipt Notification (SIARN) (See 3.5) in the inner envelope. Security-mark the inner envelope and seal with the security tape specified in the Security Equipment Guide. Address as in 3.2. See also 3.1(a)(ii); or
 - when mail is not transmitted by appropriately-screened personnel or is in a bulk shipment, use option at 3.1(a)(ii). Enclose a SIARN, then security-mark and seal the inner envelope with the security tape specified in the Security Equipment Guide. The container must be locked or sealed at the departure point and opened at the reception point (i.e. "be controlled") by appropriately-screened personnel. Address as in 3.2; or
- DFAIT Diplomatic Security Mail Service enclosed in a double envelope. Place a SIARN in the inner envelope. Security-mark the inner envelope, seal with the security tape specified in the Security Equipment Guide and address as in 3.2.

3 Detailed Specifications

3.1 Enveloping

(a) In place of a single or outer envelope, a briefcase or other container of equal or greater strength may be used. See also 3.2(a)(ii).

- (i) *When replacing a sealed envelope, the replacement container must be either locked or sealed as specified in the Security Equipment Guide.*
- (ii) *When replacing an outer envelope for information and assets designated extremely sensitive or classified secret or top secret transmitted between facilities **outside Canada**, the inner envelope must be enclosed in a locked **classified information***

dispatch case or approved equivalent container. See also 1.4 and 4.2(a).

(b) A double envelope should be used instead of a single envelope, when such packaging will better protect fragile contents (for example diskettes) or keep bulky, heavy or irregularly-shaped parcels intact.

3.2 Addressing

(a) On single envelopes and the outer jackets of double envelopes, address in a non-specific manner when possible (for example, to the department mail-room at a facility, or to a branch or section). This procedure coupled with the absence of security-markings will preserve the anonymity of the sensitive information and assets in the general mail-flow.

(i) For transmittal by the DFAIT Diplomatic Mail Services, address the outer envelope to the Manager, Mail Room Operations, DFAIT.

(ii) When a briefcase or other container is used as an outer envelope, it should be tagged with a forwarding or return office address and telephone number.

(b) Because of the need-to-know or need-to-access principles, one of the following restrictive caveats should be included when warranted on a single or an inner envelope:

(i) "To be opened only by" -- plus a position title, when only the incumbent of that position is to access the contents; or

(ii) "To be opened only by" -- plus a name, when only the identified individual is to access the contents - as in the case of personal information.

3.3 Delivery responsibility

(a) *When sensitive information and assets are transmitted via proprietary mail or messenger service, delivery personnel must ensure that a specific position incumbent or delegate receives the mail.*

(b) *The recipient of sensitive information and assets at the delivery point must ensure that the envelope or other container holding such information and assets is intact and has not been tampered with.*

3.4 Reliability of courier services

The reliability of a courier service may be established through verification with other clients, the Better Business Bureau, or the local police.

3.5 Sensitive Information and Assets Receipt Notification

Where a SIARN is required, the following format and procedures should be adopted:

(a) The receipt form should indicate the point of origin, the name of the initiating branch or office, the date of dispatch, the designation or classification level of the transferred information and assets, and any other pertinent instructions.

- (b) Forms should be individually numbered, to facilitate the audit function, and should comprise three copies, preferably colour-coded. The original and a duplicate copy should be forwarded to the recipient - inside the same double-envelope as the sensitive information and assets where feasible. The triplicate should be retained on file until the receipted original is returned.
- (c) The SIARN should request: signature of the recipient; date received; and return of the original copy by a prescribed time.
- (d) If the signed original is not returned within the prescribed time, receipt of consignment should be confirmed by the originator. The transmittal service or, subsequently, the police with jurisdiction should be alerted as required.

4 Sensitive Information and Assets at Higher Risk

4.1 General

Some sensitive information or assets at higher risk may warrant safeguards above the minimum requirements identified in this standard. *Departments must use more creative or additional safeguards to transport or transmit sensitive information and assets when warranted by their TRA.* Examples may be :

- (a) particularly sensitive, personal information concerning employees within the same department;
- (b) megabytes of sensitive information stored in a single cassette cartridge; voluminous documents packed in crates; or bulk shipments of sensitive mail;
- (c) designated information and assets concerning technical, scientific and economic matters;
- (d) classified information and assets concerning weapons technology, nuclear and biological weapons technology, COMSEC, and foreign policy; and
- (e) information and assets designated extremely sensitive or classified in the national interest sent outside of Canada. (See also 4.2).

4.2 Transport or transmittal outside Canada

- (a) When sensitive information and assets are transported or transmitted to, from, or within foreign countries and particularly in non-NATO countries, there is a higher risk of compromise by customs or other government information-gathering services. In countries where such compromise may occur, the use of the DFAIT Diplomatic Mail Services is recommended for all categories of sensitive information and assets. For advice regarding protocols used and the current threats to such information and assets while entering or circulating within foreign countries, contact the DFAIT.
- (b) When the size or composition of the sensitive information and assets precludes the use of the DFAIT Diplomatic Mail Services, contact DFAIT for guidance.

4.3 Transport or transmittal to industries outside Canada

- (a) As a result of industrial security agreements between Canada and other nations, different standards may apply to the transport or transmittal of sensitive information and assets between foreign industries under contract to departments of the Canadian Government, or between Canadian industries and the departments of foreign governments. Generally, these standards require the transfer of sensitive information and assets via established government-to-government industrial security channels.
- (b) Contact the Industrial and Corporate Security Directorate of Public Works and Government Services Canada for guidance on the transport or transmittal of this type of sensitive information and assets.

4.4 Additional safeguards

The following additional safeguards for the transport or transmittal of sensitive information and assets may be appropriate depending on the TRA:

- (a) For the lower categories of sensitive information and assets, forward as for the next higher designation or classification. (For example, forward information and assets designated low sensitive as for particularly sensitive; forward confidential information and assets as for secret);
- (b) Use the DFAIT Diplomatic Security Mail Service or Air Freight Service for the transmittal of sensitive information and assets outside Canada. See also 4.2. and 4.4(c);
- (c) For sensitive information and assets at higher risk that warrant additional safeguards, consider using any combination of the following procedures;
 - (i) double-envelope the information and assets;
 - (ii) security-mark the inner envelope;
 - (iii) security-tape the inner envelope as specified in the Security Equipment Guide (SSB/SG 20);
 - (iv) initiate a Sensitive Information and Assets Receipt Notification (See 3.5);
 - (v) use a designated information dispatch case as specified in the Security Equipment Guide (SSB/SG 20).

