Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

DECLASSIFICATION
AUTH/AUT NO. PCO - 11.8.78
NAME/NOM T.D. FINN
SIGNATURE Louise Bigue

CONFIDENTIAL

SECURITY OF INFORMATION

IN THE

PUBLIC SERVICE OF CANADA

Approved by the Security Panel

Office of the Privy Council,
November, 1956.

006888

AGC-1049_0001

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

PREFACE

1. For the purposes of this book, security means the taking of measures to prevent, or at least hinder, the collection of classified information by agents of any foreign power. These measures are also designed to prevent or hinder any unauthorized persons from having knowledge of classified information, since through ignorance, carelessness or weakness they may become channels by which classified information may reach agents of a foreign power.

2. Spies must do two things: they must collect information, and they must communicate what they have collected to their masters. All the regulations which follow are designed to prevent them from obtaining information in the first place. The reason for each regulation should therefore be apparent. Where it is not apparent the regulation must be taken on trust. Espionage has been carried out for centuries, and experts in this field have a long experience of how it can best be combatted. These regulations are an application of that experience.

3. The instructions contained in this book lay down the minimum security requirements which all departments and agencies are to enforce. Because security is largely an interdepartmental problem, the need for consistency of security procedures among all departments and agencies is paramount. Security obviously cannot be satisfactorily maintained if one department applies less effective standards than another. The instructions which this booklet contains are therefore mandatory. Security control, however, is a departmental responsibility, and therefore an additional duty rests on each department and each official to take such further measures as may in particular circumstances seem necessary to meet the individual needs of a department.

AGC-1049_0002

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

4. Many of the regulations, however, are only deterrents to espionage, for there is no security measure which can fully protect a department or agency which may number a foreign agent among its employees. For this reason they must be supplemented by the initiative, vigilance and common sense of all persons who are permitted access to classified information. All departments and agencies handling classified information are required by Cabinet Directive to appoint a security officer, whose responsibility it is to ensure that these regulations are effectively administered.

5. The principle upon which all good security must be based is that classified information should be made available only to persons who have had an appropriate security clearance and who need to have such information in the performance of their duties. It should not be made available to persons merely because of the positions they hold or the level to which they have been cleared for security. It is the responsibility of senior officers to decide which information is or is not relevant to the duties of their staff.

6. The regulations are being circulated to all departments and agencies, and may be usefully distributed to such senior officials as may require them. They are not, however, intended for distribution to all employees. The Panel has assumed that they will form the basis of departmental regulations designed to meet the particular circumstances of each department or agency.

R.B. Bryce,
Chairman of the Security Panel.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

I. - SECURITY OF DOCUMENTS

A. Definitions of Classifications

1. All official documents produced by the Canadian public service are the property of the Canadian Government. Most of these documents, together with those on loan from other governments, require some form of protection. The degree of security protection that a document requires will be indicated by a classification placed preferably in its top right-hand corner. There are four classifications which are generally recognized by the North Atlantic Treaty Organization, and they apply not only to letters, memoranda, telegrams, reports and photographs, but also to notes, rough copies, stencils, carbons, stenographers' notebooks, sketches, discs and tapes used in connection with dictating equipment, etc.

2. The following are definitions of the four classifications together with examples of their application. It is to be noted that the function of these classifications is to indicate the degree of precautionary measures which must be taken to protect the documents or other material on which they appear.

Top Secret

3. Documents, information and material are to be classified Top Secret when their security aspect is paramount, and when their unauthorized disclosure would cause exceptionally grave damage to the nation. From this general description it will be seen that the classification of Top Secret should be used only rarely. When it is used, the user should first be certain that all the special measures which are contingent upon its use are in fact fully justified. The following are examples of subjects falling within this category:

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(a) Documents or material containing plans for the defence of the nation as a whole or of strategic areas vital to its defence;

(b) Information on new and important munitions of war, including important scientific and technical developments directly connected with the defence of the nation;

(c) Detailed information on new or proposed defence alliances, and on the defence plans of allied nations.

Secret

4. Documents, information and material are to be classified Secret when their unauthorized disclosure would endanger national security, cause serious injury to the interests or prestige of the nation, or would be of substantial advantage to a foreign power. The following are examples of subjects falling within this category:

(a) Minutes or records of discussions of Cabinet or Cabinet Committees;

(b) Documents or material containing plans for the defence of areas and installations of other than vital strategic importance;

(c) Documents or material directly pertaining to current and important negotiations with foreign powers;

(d) Particulars of the national budget prior to its official release;

AGC-1049_0005

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(e) Information about foreign powers, the value of which lies in concealing our possession of it;

(f) Information about new and important scientific and technical developments pertaining to national defence;

(g) Information about the identity or composition of scientific or military units employed on operations involving techniques, the knowledge of which would be of substantial value to a foreign power.

Confidential *

5. Documents, information and material are to be classified Confidential when their unauthorized disclosure would be prejudicial to the interests or prestige of the nation, would cause damage to an individual, and would be of advantage to a foreign power. The following are examples of subjects falling within this category:

(a) Information of a personal or disciplinary nature which should be protected for administrative reasons;

(b) Minutes or records of discussions of interdepartmental committees when the content of such minutes or records does not fall within a higher category;

* Documents which are 'Confidential' not in the sense of a security classification as used here, but merely private and personal, should be marked "In Confidence" or "Private and Personal". These designations can be used, for instance, on certain letters to provincial governments or to commercial organizations where the contents are for the private information of the addressee and must not be made public, but do not need the protection given to a document bearing the security classification 'Confidential'.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(c) Political and economic reports which would be of advantage to a foreign power but which do not fall in the Secret category;

(d) Private views of officials on public events which are not intended to be disclosed.

Restricted

6. Documents, information and material are to be classified Restricted when they should not be published or communicated to anyone except for official purposes, and when they are not classified in any of the three previous categories.

B. General Principles Governing Classification of Documents

7. Strict adherence to the rules governing the classification of documents is the basis of good security. All classified documents must bear the security marking preferably on the top right-hand corner of the page. Classified documents include, in addition to letters, memoranda, telegrams, reports and photographs, notes, rough copies, stencils, carbons, stenographers' notebooks, sketches, discs and tapes used in connection with dictating equipment, etc.

8. The following important principles should be borne in mind in giving a classification to a document:

(a) Each document will be classified on its merits by reference to its contents and their implications and not by reference

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

to an automatic test, e.g. the classification of other documents in the same series. Covering letters or reference slips will bear the same classification as the document to which they are appended, and will indicate how they should be classified when appended documents are removed. A reference to a classified document will bear the same classification as the original only if the contents of the original are made clear in the reference. An extract from a classified document will bear the same classification as the original, except where the extract is obviously of a lower category. Where there is doubt, the originator should be consulted.

(b) It should be borne in mind that the source of the information contained in a document may justify a higher classification than the information taken by itself would at first seem to warrant, e.g. Confidential information obtained from a very delicate source may justify the classification of a document as Secret. That is, the process by which the information was obtained may require more protection than the information itself.

(c) The tendency to give too high a classification to information is a natural one, but the result is to clog the

AGC-1049_0008

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

the machinery for dealing with documents and to allow personnel to become so familiar with handling highly classified material that the significance of the classification becomes obscured, particularly if persons handling the material recognize that it is over-classified.

(d) The classification appropriate to a document may alter with the passage of time, and departments should arrange to review classified documents as and when required. Documents received from other departments should not be downgraded without the approval of the originating department. In the case of reports from intelligence sources, factors other than the contents of the report may need to be considered. When it has been decided to regrade a document or when notification has been received from an originating department about regrading one of their documents, the old security classification should be deleted in ink and the new one substituted. The deletion should be signed and dated by the officer responsible and a note made of any documentary authority for it. It is strongly recommended that the originating department indicate wherever possible, either at the time of issue or later, that a document may be downgraded after a given date or event.

AGC-1049_0009

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

C. Preparation of Classified Documents

9. During the course of preparation of a classified document a number of auxiliary papers and items which require protection may accumulate. These will usually be in the form of notes, rough copies, stencils, carbons, stenographers' notebooks, sketches, discs and tapes used in connection with dictating equipment, etc. An important document may frequently pass through a number of draft typescripts before it reaches its final form. All these auxiliary papers should be classified when they are made and given the degree of protection they require.

10. Documents in their final form should bear a clear classification preferably in the upper right-hand corner of each page. In addition all Top Secret documents should bear the classification at both the top and bottom of each page, and a copy number should be shown on the first page or title sheet. A record should be maintained of the disposition of each numbered copy of all Top Secret documents.

11. Only the required number of copies of documents of all classifications should be made. When common sense requires that a few additional spare copies should be kept in reserve, a note should be made of the number. Once it is apparent that no further copies will be called for, all the spares should be destroyed, if the document originated in the department. Otherwise, the originating department should be consulted before spare copies are destroyed. A Top Secret document should never be copied in extenso without the consent of the originator.

12. When the final version of a classified document is completed, all the auxiliary papers referred to above should be destroyed in accordance with the regulation set out in section I.H. below.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

D. Transmission of Classified Documents

13. One of the weakest points in any security system lies in its communications. When documents are being transmitted from one point to another it is difficult to give them the degree of protection they require. This weakness is particularly aggravated when they are given to a public communications system or placed in the care of persons whose reliability may not be assured.

14. For this reason documents classified Top Secret, Secret and Confidential should be sent within or without Canada by an officially sealed diplomatic or service bag, or by safe hand of messenger or employees who have been given an adequate security clearance in accordance with the current Cabinet Directive on security investigation. Documents classified Restricted which are to be sent between points within Canada may be committed to the open mail, provided they are packaged in two envelopes.

15. However, because of the great distances which classified documents must sometimes travel, and because of the expenditures involved in maintaining a messenger or courier service, Registered Mail may be used for transmitting classified documents under the following circumstances:

(a) For the transmission within a Canadian city or locality, except within Ottawa, of documents classified Confidential when there is no material of a higher classification and the small volume of Confidential material does not justify the use of a messenger service. Ottawa has been excepted because the great bulk of classified information passing between departments and agencies within the Capital requires

AGC-1049_0011

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

the maintenance of messenger services adequate to make the use of Registered Mail unjustified;

(b) For the transmission within Canada (but not within a city or locality) of documents classified Secret or Confidential when adequate courier services do not exist;

(c) For the transmission, by Air Mail only, between Canada, the United Kingdom and the United States of documents classified Confidential or Restricted when no adequate diplomatic or service bag capable of handling the volume is available;

(d) For the transmission between points lying entirely within Australia, New Zealand, South Africa, the United Kingdom or the United States of documents classified Confidential or Restricted when no adequate diplomatic or service bag is available.

16. It is recognized that some departments and agencies may face exceptional problems of communication, particularly with respect to Top Secret material, which will require special arrangements. These may be made only with the concurrence of the Chairman of the Security Panel, who will refer difficult matters to the Panel itself.

E. Packaging of Classified Documents

17. It is important to ensure that classified documents in transit be kept from the eyes of unauthorized persons, and they should therefore be covered at all times during

AGC-1049_0012

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

transmission. The extent and nature of the cover will be dictated by the security risk involved in the method of transmission which is to be used. Obviously the security risk involved in transmitting classified documents from office to office within a building is not as great as that involved in transmission from building to building, from city to city within Canada, or outside the country. Therefore, in each of these cases, certain basic rules must be borne in mind.

18. Departments and agencies are asked to note that all "By Hand" deliveries should be enclosed in a bag or box which can be securely locked, even though the documents themselves may be enclosed in double envelopes. The purpose of this measure is to prevent envelopes being inadvertently dropped or otherwise mislaid in transit by hurrying messengers. This extra cover is obviously not required for documents enclosed in an officially sealed diplomatic or service bag.

19. When documents are being transmitted which contain highly sensitive information or information which would cause embarrassment in the wrong hands, it is a useful measure to add to the address the words "To be opened only by.....".

20. It is also to be noted that whenever sealing wax is used, it must be stamped with an official stamp or seal, which must at no time be accessible to other than authorized staff. In order to avoid any possible confusion, the word "sealed" in the following paragraphs means "stuck down", and should be distinguished from "sealed with sealing wax".

21. In accordance with these rules and principles, the packaging of classified documents will be as follows:

AGC-1049_0013

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(a) From Office to Office within a Building

(i) A document classified Top Secret or Secret being sent by messenger from office to office within a building must be in a sealed and properly addressed envelope bearing the security classification of the document, or in a locked container;

(ii) A document classified Confidential being sent by messenger from office to office within a building should be in a closed and properly addressed envelope bearing the security classification of the document, or in a closed container;

(iii) Within restricted areas inside a building (see para. 44 below), the manner in which classified documents are sent from office to office may be left to the discretion of the security officer.

(b) From Building to Building within a City or Locality

(i) A document classified Top Secret or Secret being sent from one building to another within a city or locality must be in two envelopes. The inner envelope must bear the correct address and the security classification of the document it contains and must be sealed with sealing wax. The outer envelope must not under any circumstances bear a

AGC-1049_0014

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

security classification but should be properly addressed and marked "By Hand";

(ii) A document classified Confidential being sent by messenger from building to building within a city or locality must be in a sealed envelope bearing the correct address and the security classification, and must be marked "By Hand";

(iii) A document classified Confidential being sent by Registered Mail within a city or locality must be in two envelopes. The inner envelope must bear the correct address and the security classification of the document it contains. The outer envelope must not under any circumstances bear the security classification, but must be clearly marked "Registered Mail".

(c) From City to City within Canada

(i) A document classified Top Secret or Secret being sent from city to city within Canada by messenger or courier must be in an envelope sealed with sealing wax, bearing the correct address and the security classification of the document it contains and marked "By Hand". The envelope must be in a securely locked bag or container bearing the departmental title or other adequate indication of government ownership, and the bag must not be opened en route;

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(ii) A document classified Confidential being sent from city to city within Canada by messenger or courier must be packaged as in (c)(i) above, except that the inner envelope need not be sealed with sealing wax;

(iii) A document classified Secret being sent from city to city within Canada by Registered Mail must be in two envelopes. The inner envelope must bear the correct address and the security classification of the document it contains, and must be sealed with sealing wax. The outer envelope must not under any circumstances bear the security classification but must be clearly marked "Registered Mail";

(iv) A document classified Confidential being sent from city to city within Canada by Registered Mail must be packaged as in (c) (iii) above, except that the inner envelope need not be sealed with sealing wax.

(d) Outside Canada

(i) A document classified Top Secret or Secret being sent outside Canada by officially sealed diplomatic or service bag must be in an envelope sealed with sealing wax bearing the security classification of the document it contains and the correct address;

(ii) A document classified Confidential being sent outside Canada by officially sealed

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

diplomatic or service bag must be in a sealed envelope bearing the classification of the document it contains and the correct address;

(iii) A document classified Confidential or Restricted being sent outside Canada by Registered Mail (see sub-paragraphs 15(d) and (e) above) must be enclosed in two envelopes. The inner envelope must bear the security classification of the document it contains and the correct address and must be sealed with sealing wax. The outer envelope must not under any circumstances bear a security classification but should be clearly marked "Registered Mail".

F. Receipts

22. When a department or agency sends a classified document or classified material to another office under the safeguards set out in sections D and E, it is desirable whenever possible to have assurance that the document or material has arrived at its destination safely. Assurance of this kind can be provided by a system of receipts.

23. However, in view of the bulk of classified material passing daily from office to office within the government service, it is clearly impractical and uneconomical to require a signed receipt in every case. It is, however, mandatory that documents or material classified Top Secret and being sent outside a building be accompanied by a receipt which should be signed by

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

the recipient and returned to the sender without delay. If a receipt for a Top Secret document is not received within a reasonable length of time the originator should immediately make enquiries as to the whereabouts of the document. It is recommended that departments and agencies use a similar receipt system for Top Secret documents when they are moved from office to office within a building.

24. Receipts for classified documents should be made in at least two copies in order that a carbon copy may be retained on file as a record of receipted documents sent out, and against which the original copy of the receipt may be checked when it is returned.

25. For documents classified Top Secret, Secret or Confidential being sent outside a building by safe hand, it is strongly recommended that departments and agencies require a number to be allotted to each envelope or package and have the number entered in a book in which the signature of the recipient is to be written opposite each item. The head messenger, or another responsible person designated by the security officer, should check the signature after each delivery. Only if a system of this kind is followed is it possible to trace a lost document.

G. Custody of Classified Documents

26. Classified documents should be stored in containers which provide a degree of protection suitable to the level of classification. The degree of protection required from the container will in turn depend upon the general security of the premises and the nature of the locality in which they stand. For instance, in a building with barred windows or other perimeter protection where there is a twenty-four hour guard system a

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

container providing only a moderate degree of security might be acceptable but would be considered inadequate in an entirely unprotected building.

27. Therefore no hard and fast rules can be laid down concerning the use of containers, but it is mandatory that departments and agencies use only equipment of a pattern that has been tested by the R.C.M.Police laboratories and approved by the Security Panel. Lists of this equipment have been provided to security officers throughout the government service.

28. Advice as to the security standard of equipment desirable in any particular circumstances is immediately available to departments and agencies in Ottawa from the Lock Inspection and Maintenance Team provided by the R.C.M.Police laboratories. This team can be called in for consultation by writing to the Officer-in-Charge, Crime Detection Laboratory, R.C.M.Police, Ottawa. The team will also provide a regular lock maintenance service for containers on request.

29. Further information on the security of safe dial combinations and keys is to be found in paragraphs 42-44 below.

H. Destruction of Classified Documents

30. It is essential that any material containing classified information be completely destroyed when it is of no further use. It is equally important that such material be given adequate protection until it is actually destroyed. The manner in which this protection is provided for classified waste must be determined by the general security of the premises, but the following minimum standards are provided for the guidance of departments and agencies:

AGC-1049_0019

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(a) Classified waste must be placed in plainly marked receptacles used solely for this purpose. Wire baskets must not be used;

(b) During working hours classified waste should not at any time be left unattended in unlocked rooms or offices;

(c) Classified waste should be gathered at the end of every day by a responsible person or persons who have been given an adequate security clearance, and should be stored in a securely locked steel container until it can be destroyed;

(d) Care must be taken to safeguard classified waste while it is in transit from a place of storage to the destruction facilities.

31. The destruction of classified waste must be accomplished under the supervision of a competent person who has been given an adequate security clearance. Burning or pulping are preferred methods but shredders approved and listed by the Security Sub-Panel after testing by the R.C.M. Police may be used without further recourse to burning or pulping where circumstances warrant. If papers are burned they must be reduced to ashes unrecognizable as papers. It is strongly recommended that a signed certificate of destruction should be obtained on each occasion.

32. Recording discs and tapes containing classified information should be periodically cleared if they are to be used again, and should be kept in a safe place at all times.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

II. - SECURITY OF STAFF

A. Security Enquiries

33. Security in the public service of Canada is essentially a part of good administration, which may be placed in jeopardy either by persons who are disloyal or by persons who are unreliable because of defects in their character. In order that departments and agencies of the government may be properly administered, department and agency heads must satisfy themselves as to the suitability of personnel before they are employed.

34. It remains an essential of Canadian security policy that a person who is a member of a Communist party, or a person who by his words or actions consistently shows himself to believe in Soviet Communism, or in any other ideology which advocates the overthrow of government by force, should not when known be permitted to enter the public service. Such persons discovered within the public service must not be allowed access to classified information. It is also essential that persons whose defects in character may lead to indiscretion or dishonesty, or may make them likely subjects of blackmail, be denied access to classified information.

35. For these reasons it is necessary for the government to make certain enquiries into the background of persons who are to be given access to classified information for which the government is responsible. The methods by which enquiries are to be made have been laid down in a Cabinet Directive.

B. Administration of Oaths

36. It is required under the Civil Service Act that every deputy head, officer, clerk and employee in the Civil Service

AGC-1049_0021

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

take and subscribe to the Oath of Allegiance and the Oath of Office and Secrecy, subject to certain exemptions laid down by Order-in-Council. In addition, before any person is given access to classified information, each department and agency is asked to ensure that the employee signs a declaration indicating that his or her attention has been drawn to the provisions of the Official Secrets Act. The signing of this declaration in no way obviates the necessity for an adequate security clearance. A specimen declaration is as follows:

> My attention has been drawn to the provisions of the Official Secrets Act, 1939, and I am fully aware of the serious consequences which may follow any breach of such provisions.
>
> I undertake not to make any disclosure of classified information gained by me as a result of my employment to any person not normally authorized to receive it, orally or in writing, without the previous sanction of my superior officer in the department.
>
> I understand also that these provisions apply not only during the period of employment but also after employment with the department has ceased.
>
> I appreciate that all the classified information which I may acquire or to which I may have access either during or subsequent to my employment is information which is covered by Section 4 of the Official Secrets Act, 1939, and that it would be a contravention of this Act for me after I have left the Canadian government service -
>
> (a) to publish without lawful authority any such information in any form, whether orally or in any document, article, book, play, film or otherwise, or
>
> (b) to communicate without lawful authority any such information to any other person whether or not such person is or has been employed in the service of the government.
>
> I further undertake, on leaving the department, to surrender any sketch, plan, model, article, note or document made or acquired by me in the course of my official duties, save such as I have been duly authorized to retain by my superior officer in the department.

Signed_____

Witnessed_____ Date_____

AGC-1049_0022

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

37. In order that the individual might be impressed with the need of being aware of security precautions, the administration of oaths should not be done in a routine or casual manner. The departmental or agency security officer should ensure that the implications of the procedures and the basic importance of an awareness of security are clearly explained to the employee. Also, a record should be kept of the oaths and declarations signed by the employee.

C. Security Training

38. Security regulations and procedures are often regarded as a tiresome necessity. Because of their restrictive nature and because they are normally extraneous to the work upon which a person is engaged, security regulations tend to be read and forgotten.

39. When new employees are engaged, security regulations and practices should be thoroughly explained, together with the reasons behind them. It should be impressed upon them that the observance of these regulations is their personal responsibility and that the security of the department as a whole is only as good as the security of each member. Use should be made whenever possible of the "Memorandum on Security for Clerical Staff" issued by the Security Panel on October 30th, 1952.

40. Although it is not possible to give formal training in security procedures to all members of the public service, periodic courses of lectures are held for the benefit of all departmental and agency security officers, who may be consulted by personnel on matters of security. Security officers will also find it a useful practice to circulate departmental security regulations periodically to all personnel and to conduct lectures

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

from time to time on various security subjects. If security matters can be put to personnel as matters of interest rather than as an imposition of restrictions, departmental and agency security officers will find their tasks a good deal lighter.

III. - SECURITY OF OFFICES AND BUILDINGS

A. Security of Offices

41. Public servants handling classified material must be certain that their office doors are securely locked or that unauthorized entry to the office is otherwise prevented whenever the office is unoccupied even for the briefest times during working hours. Advice as to locks most appropriate in any given circumstances may be obtained from the Lock Inspection and Maintenance Team of the R.C.M.Police (see paragraph 28 above). Appropriate care should be taken of windows in offices on the ground floor. Doors and windows in rooms housing classified material must be securely locked at night, and all classified material, including classified waste, should be locked away in approved security containers. (see section I.G. above).

42. The dial combinations of security containers within offices should be changed at least every six months, on the departure of staff who have had knowledge of combinations, or when the combinations may have been compromised.

43. The strictest control must be maintained over the use and storage of keys. They should be issued only to persons who have been cleared for security and should, if possible, be locked in a secure central container or left in the custody of

AGC-1049_0024

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

a guard when not in use at night. An impression of a key can be made very quickly and simply, and cases are known where very important information has been compromised through the improper control of keys. Keys permitting access to the offices may, if essential, be retained by responsible persons and a list of all persons holding keys should be maintained.

44. It is recognized that some offices containing classified material must be open, to some extent at least, to the public during working hours. For this reason, it is recommended that wherever possible a restricted area should be set aside within the premises to contain as much of the classified material as normal working conditions may permit. In particular, registries and communications centres should be within this area. There should, if possible, be only one entrance to this area which should be shut off by a locking door. Keys to this door should be held only by cleared personnel who will need to enter the area during the course of their duties. Any other entrances to the area should, if possible, be kept permanently locked and the keys stored in a safe place. Under any circumstances it is essential to ensure that visitors (see paragraphs 54 - 56 below) are never left unattended in an area where classified documents are openly available. Cleaning staff should only be permitted in restricted areas under supervision. Cleaning staff working in offices containing Top Secret material should have been subject to a satisfactory security clearance provided by the Department of Public Works.

45. Persons who have not received, and do not require, a security clearance, should not normally be permitted to work in rooms with cleared personnel handling classified information. Where accommodation is such that complete segregation is impossible, it is mandatory that classified material never be left unattended by cleared personnel or made accessible to unauthorized personnel.

AGC-1049_0025

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

B. Security of Buildings

46. It is important that adequate measures are taken to prevent illicit entry into a government building which houses classified material. The extent of these measures will depend upon the nature of the guard system in force. (See paragraphs 48-53 below). However, as a general rule, all outside doors, windows and other means of entry should be fitted with approved locks, and protective equipment may have to be used on windows accessible from the ground or from adjacent structures, depending upon the kind of information which it is necessary to protect. Certain departments and agencies may find it advisable to install an alarm system, which may protect the whole building, or an area in which a large amount of classified material is stored. The installation of an alarm system must be on the authorization of the department or agency head, and it must be efficiently and consistently serviced to be of any use.

47. Keys to the outside of buildings may, if essential, be retained by responsible persons whose numbers should be strictly limited. A list of such persons should be maintained.

48. Security guards drawn from the Canadian Corps of Commissionaires are employed by a number of departments and agencies for duty in buildings exclusively occupied by a particular department or agency. In such cases the strength of guard details, the hours of duty and the standing orders under which the guards operate are the responsibility of the department or agency concerned.

49. In buildings containing offices of more than one department or agency, the R.C.M.Police are responsible for the administrative control of Commissionaires employed as security guards, and departments and agencies who share premises requiring

AGC-1049_0026

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

security guards may make the necessary arrangements with the Commissioner of the R.C.M.Police. However, whether or not security guards are employed, it is important that departments and agencies realize that they are at all times responsible for overall security in their buildings.

50. All guards employed in Canadian government buildings where classified information is stored, whether they are drawn from the Canadian Corps of Commissionaires or are privately employed, should have received a satisfactory security clearance. Where the guards are the responsibility of a department or agency, the security officer or a responsible person designated by him should from time to time make a spot check at night to ensure that the guards are efficient and alert.

51. Where guards are employed during the day on entrances to buildings housing classified information they should normally permit entry of staff by recognition or on production of a building pass card. (For the entry of visitors see paragraph 54 below). Guards should be provided with a specimen pass card in all cases. It is strongly recommended that departments and agencies use the standard pass card, renewable annually, approved by the Security Sub-Panel. This provides a minimum standard. Additional measures, such as the issuance of full identification cards, may be desirable in certain buildings.

52. In many cases during the day time it will not be possible to employ guards on all entrances to buildings. In these cases security must rest with authorized staff within offices who must ensure that unauthorized persons are not permitted to see classified information or overhear conversations dealing with classified information.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

53. During the quiet hours access to buildings should normally be limited to one entrance only, which is to be supervised by a night guard. All other entrances should be securely locked. The night guard should permit entry only on production of a building pass card. It may be desirable for the guard to be provided with a list of staff permitted to enter at certain hours. In all cases the guard should make a note of the name of a person admitted to a building together with the times of arrival and departure. These lists should be examined at least weekly by the departmental or agency security officer.

54. The control of visitors to buildings containing classified information will depend upon the level of security required and the number and nature of visitors. Where the work of the office is such that it has been found desirable to permit entry during working hours only at one entrance under the supervision of a guard, visitors should be required at least to identify themselves and state their business. It is for a departmental or agency security officer to decide whether an escort system within the building is desirable.

55. In buildings where there are entrances without guards during working hours the control of visitors must again rest with the presence of authorized staff within the offices. Visitors must not be permitted to remain unattended in rooms where classified information is open to them.

56. Entry during the quiet hours of visitors to buildings housing classified information should be permitted by night guards only on the instructions of a responsible person who is present to receive them.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

IV - COMMUNICATIONS SECURITY

A. Definition and Requirement

57. Communications security comprises the measures instituted to protect our national communications from interception or monitoring by unauthorized persons. Although complete protection cannot be realized, the aim of communications security is to reduce to a minimum the amount of information which an unauthorized person can derive from listening to and studying the two types of transmissions: the transmission of language messages over radio or wire circuits, commonly known as communications transmissions; and the emission of electronic impulses (such as radar signals) which do not contain language messages, commonly known as non-communications or electronic transmissions.

58. Communications security requirements may be considered under three headings: Cryptographic Security, Transmission Security and Telephone Security.

B. Cryptographic Security

59. All classified information transmitted by government departments and agencies by any communications system must be protected by means of a cryptographic system approved by the Communications-Electronic Security Policy Committee after evaluation of its effectiveness and of the methods of employing the ciphers. Under no circumstances may classified information be transmitted by means of any electrical communications system, whether radio, land-line or submarine cable, in clear or in "commercial code", that is, a code designed to provide privacy or brevity rather than security.

60. Departments which employ "commercial codes" for the transmission of unclassified administrative information must bear in mind that no element of security is obtained by their use. Information and advice as to the availability and use both of approved ciphers and of "commercial codes" may be obtained from the Communications-Electronic Security Policy Committee which can be consulted through the Secretary of the Security Panel.

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

C. Transmission Security

61. Security of communications transmissions depends on strict adherence to approved communications and message handling procedures, and on careful attention to the accurate classification of messages. Particular care must be taken to limit to a minimum the number of plain language and unclassified messages. This is necessary because a large number of individual messages, each of which may appear harmless in isolation, may over an extended period of time reveal useful information on classified subjects. Replies or references to classified messages, though they may contain no classified information themselves, must not be transmitted in unclassified form, since they can often be related to the messages to which they refer, and thus may provide some indication of the contents of the original classified messages.

62. Care must be exercised with regard to non-communications transmissions as well as to communications transmissions, since valuable information can be obtained through their interception. For instance, electronic systems such as navigational aids and radars may emit signals which reveal the technical characteristics of the basic equipment. For this reason careful consideration should be given to the location, physical security arrangements and operation of establishments which might be engaged in the development, production or operation of any such electronic systems.

63. Interception and monitoring operations directed against communications and non-communications transmissions may be carried out by unauthorized persons from fixed or mobile establishments located near the point of transmission. Therefore, in certain instances it may be advisable for the department or agency concerned, before undertaking the installation of radio communications systems or when planning classified electronic projects, to consult the Communications-Electronic Security Policy Committee (CSPC) through the Secretary of the Security Panel, concerning the security aspects of such installations and projects.

AGC-1049_0030

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

D. Telephone Security

64. It must be assumed that, pending the availability of suitable speech secrecy equipment, telephone communications are insecure, whether the channels used are routed by landline, microwave radio, submarine cable, or any combination of these. Telephone conversations can be intercepted either by casual eavesdropping at relay or switching centres, or as a result of deliberate monitoring of the circuit.

65. At the present time the most effective security protection for telephone communications is the vigilance of the persons transmitting the messages. The telephone must not be used to communicate classified information, except in an emergency when the need for speed may override the security requirement.

AGC-1049_0031

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

V. - SECURITY OF CLASSIFIED INFORMATION ENTRUSTED TO PERSONS OUTSIDE THE PUBLIC SERVICE

61. From time to time classified material must be given to non-governmental organizations or to private individuals - particularly in the defence industry. Since classified material must be protected wherever it may be, the government's security regulations must apply with equal force in these cases.

62. Therefore a department or agency supplying classified material to persons outside the public service must ensure that the persons concerned are loyal and dependable, that they are fully instructed in the principles of security, that adequate security measures are taken, and that approved equipment is available.

VI. - SECURITY OF CLASSIFIED INFORMATION ENTRUSTED TO OFFICIALS OVERNIGHT

63. It is realized that it will sometimes be necessary for officials to work on classified documents at their homes in the evening or on weekends. Because of the obvious dangers to security inherent in this practice, it is strongly urged that it be limited to as few officers as possible, and that they are thoroughly instructed in all the principles set out in this booklet, particularly those concerning the preparation, packaging, transmission, custody and destruction of classified documents. In addition, the following general rules should be strictly adhered to:

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(a) Documents to be taken home should be carried at all times in a locked container;

(b) The exact contents of the container should be known to the officer removing documents. If there are any classified documents, a brief record of them should be made and kept in the office;

(c) In transit, and particularly in public conveyances, the container must never be placed in a luggage rack or under a seat, but should be in the officer's physical possession at all times;

(d) In private automobiles, the container must at all times be in the possession of the officer responsible, and should not at any time be left in the automobile, even if it is locked;

(e) At the officer's residence, the container should be placed out of sight in a safe place, and under no circumstances should the container be left where it is availsble to children, tradesmen or casual visitors;

(f) After the officer has completed his evening's work, all the documents should be locked in the container and stored in a safe place. The officer responsible should not leave the house during the evening;

(g) Before leaving for work in the morning, the officer should check the contents of his briefcase or other container, in order to ensure that all the documents he removed from his office are accounted for;

AGC-1049_0033

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

(h) On arrival at the office, all the documents should be removed from the container, checked against the record of removal and placed in proper custody.

Departments and agencies are reminded that even if the above procedures are followed there are a great many dangers in removing documents from their proper custody overnight, and the practice should be strictly limited.

VII. - BREACHES OF SECURITY

69 ~~64~~. No security system can be proof against foreign agents, against foolishness or against negligence. But when security is compromised, the existence of an efficient security system can assist investigation by bringing the security breach to early notice and by immediately narrowing the field of enquiry. The purpose of an enquiry, when a breach has occurred, should be first to find out what happened and then to minimize the damage and to prevent a recurrence.

70 ~~65~~. As a first step it should be impressed upon all persons handling classified information that any breach of security should as a matter of honour be reported to the security officer immediately it comes to notice. The reason for this is that it is frequently impossible to determine how a breach of security occurred after an interval of time has elapsed.

71 ~~66~~. When a security breach is reported, a security officer should immediately gather all the facts of the matter in order to determine whether or not there is any indication of

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

malicious intent on the part of persons who may be involved. If there is such an indication, the security officer should immediately turn the investigation over to Special Branch, R.C.M.Police, and should take every possible precaution to ensure that the person or persons suspected are not alerted.

72 ~~67~~. If a security breach appears to be the result of foolishness or negligence, a security officer may wish to consider if the extent of the investigation is likely to be such that the help of Special Branch, R.C.M.Police, should be sought. In any case, if Special Branch is to be called in it is desirable that this should be done in the early stages of the investigation.

73 ~~68~~. While an investigation of a security breach is being carried out, thought should be given to what steps may be taken to minimize the damage which may have been done. An assessment should be made of the information which has leaked, other departments concerned should be consulted and whatever remedial measures are possible should be taken. Where compromise is actual or suspected, the department or agency with which the information originated should be informed.

74 ~~69~~. Each incident should be regarded not only as requiring investigation in itself but also as a means of drawing lessons for the future; as showing where the security system of a department or agency may be defective, or as indicating failure by an individual to observe the regulations. In every case the lesson should be brought home to the individual responsible, and if there has been serious negligence the matter should be brought before the head of the department or agency.

75 ~~70~~. Where the lesson to be learned from a security breach may have a general application to security throughout

AGC-1049_0035

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

the public service, an account of the matter should be forwarded to the Secretary of the Security Panel who may wish to pass the information on in general terms to other departments and agencies.

- - - - - - - - - - -

AGC-1049_0036

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

I N D E X

(References in Roman numbers and /or letters are to Sections; all other references are to paragraphs).

006924

AGC-1049_0037

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

006925

AGC-1049_0038

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

006926

AGC-1049_0039

Document disclosed under the *Access to Information Act*
Document divulgué en vertu de la *Loi sur l'accès à l'information*

Privy Council Office,
Ottawa, October, 1956.

AGC-1049_0040