

//

CI No. 205

CONFIDENTIAL

BOOKLET ON SECURITY

prepared by

THE SECURITY PANEL

for use by

**Departments and Agencies of
The Canadian Government**

**This document is the property of the Government
of Canada**

MAY, 1947

004345

AGC-1012_0001

OP No.

CONFIDENTIAL

BOOKLET ON SECURITY

prepared by

THE SECURITY PANEL

for use by

**Departments and Agencies of
The Canadian Government**

**This document is the property of the Government
of Canada**

MAY, 1947

004346

Booklet on Security
prepared by
the Security Panel
for use by
Departments and Agencies of the Canadian Government

PREFACE

Security means the taking of all measures likely to prevent or impede the transmission of information to unauthorized persons.

During the period of hostilities the urgent need for security was generally recognized, but the reasons for maintaining an equally high standard now are not at first so obvious. It will, however, be readily accepted that improper disclosures may prejudice the interests of the Canadian government, and, on occasion, other governments with which negotiations are being conducted. In some ways more care is required at the present time than during hostilities: not only because of the carelessness which follows the ending of the emergency, but for other reasons as well. The protective measures embodied in censorship and other provisions of the Defence of Canada Regulations are no longer in force. On the other hand, the recent revelations of the existence of espionage show that organized attempts are made to secure intelligence. It may be added that any government official may also reveal confidential information unwittingly.

With these circumstances in mind the Security Panel, which was constituted by Cabinet decision of May 22nd, 1946, made the study of security rules one of its first duties. The present booklet draws attention to existing regulations which are mandatory for all government departments and agencies. Various aspects of security are examined either with the purpose of giving further explanation of the government rules, or of giving advice on problems not covered by such rules.

Security control must of necessity be a departmental responsibility, and can be discharged effectively only by the application of instructions designed to meet the individual needs of a department. It is believed that this booklet will cover most of the security problems that will arise, and that rules no less strict than those suggested here will be found necessary. It is also true, however, that a duty rests with each department and each official to take such other measures as may in particular circumstances appear necessary; and in general to exercise

...vigilance and common sense in the observance of major and minor precautions.

For government officials who have no occasion to study the problem in detail rules of security must be taken on faith. The subject is a technical one, and the defensive measures suggested are drawn up in the light of known risks. Perhaps the chief danger to security is the individual who, without expert knowledge, is prepared himself to assess the needs and the risks without reference to the findings of the specialists.

This pamphlet is being sent to all departments and agencies, and may usefully be distributed to such senior officials as may require it. It is not, however, intended for distribution to all employees. Rather the Panel has assumed that it will form the basis of departmental regulations designed from time to time to meet the particular circumstances of each department or agency. The booklet itself is, of course, a confidential document.

The Security Panel will make a continued study of this subject, and will welcome suggestions or requests for advice from departments, either through their security officers, where such have been appointed, or from other responsible officials.

A. D. P. HEENEY,
Chairman, Security Panel.

Privy Council Office,
May, 1947.

I N D E X

| PREFACE | PAGE |
|--|------|
| I. SECURITY MEASURES IN RELATION TO DOCUMENTS | |
| Classification of Documents | 5 |
| Custody and Transmission of Classified Documents | 6 |
| Typing and Reproduction Arrangements | 6 |
| Disposal of Classified Waste | 7 |
| II. SUPERVISION OF STAFF ENGAGED IN WORK OF A SECRET NATURE | |
| Security Enquiries | 7 |
| Declarations Under the Official Secrets Act..... | 7 |
| Security Training | 8 |
| III. PHYSICAL SECURITY OF BUILDINGS | |
| Guards | 9 |
| Visitors | 9 |
| Identification | 9 |
| Internal Arrangements — Staff | 10 |
| Internal Arrangements — Offices | 11 |
| IV. TELEPHONE SECURITY | |
| Internal Telephones | 11 |
| External Telephones — General | 12 |
| External Telephones — Radio | 12 |
| V. CYPHER SECURITY | |
| Security Markings on Messages | 13 |
| Cypher, Code or Plain Language | 13 |
| Marking of Messages by Method of Transmission | 13 |
| Multiple Address Messages | 14 |
| Plain Language or Literal Texts | 15 |

A P P E N D I C E S

| | |
|---|----|
| “A” Security Measures in Relation to Documents..... | 16 |
| “B” Regulations Concerning Oath of Secrecy, etc..... | 21 |
| “C” Guarding and Security of Departmental Buildings | 23 |

SECURITY MEASURES IN RELATION TO DOCUMENTS

Classification of Documents

1. During the war the Canadian government adhered to an agreement between the United Kingdom and United States governments concerning the classification of documents. This agreement, which is still in effect, provided for four security categories — viz.: Top Secret, Secret, Confidential and Restricted. The regulations concerning the use of these classifications appear at Appendix “A”.

2. Strict adherence to the rules governing the classification of documents is the basis of good security. A tendency to give too high a classification to information is a natural one. But the result is almost as unfortunate as the failure to classify information at all. A general tendency to “over-classify” will result in the clogging of the machinery for dealing with documents and consequent weakening of the system.

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

- (a) a document should be classified on its own merits — i.e. by reference to its contents and their implications and *not* by reference to an automatic test. For example, the classification of a document to conform to other documents in the same series or because it happens to be a part of a classified file is wrong. On the other hand, a file containing classified documents should be given the classification of the document bearing the highest classification in the file;
- (b) the primary purpose of the document is not always the governing factor in deciding its classification. If classified material is referred to in the document under consideration, the document should normally bear the same security marking — e.g. verbatim quotation of decyphered material which might compromise the cypher if it were published; and
- (c) documents do not normally maintain the same degree of secrecy after a lapse of time. It is important, therefore, to keep the classification of documents under constant review and to downgrade them whenever the necessity for their continued protection has ceased. As is explained in the regulations, the decision on this matter rests with the originator. (Cypher telegrams are an exception to this rule; see paragraph 56).

Custody and Transmission of Classified Documents

4. The regulations concerning the custody and transmission of classified documents appear at Appendix "A". These regulations are not necessarily exhaustive, but contain safeguards which are considered to be universally applicable. Attention is drawn, in particular, to the paragraphs concerning the transmission and custody of Top Secret and Secret documents. It is important that the circulation of classified documents should be limited to those officers who require them for the efficient performance of their duties, and disclosure should not be made to any person solely because of his rank or office.

5. All classified matter should be kept under lock and key. The common practice of leaving keys of cabinets in unlocked drawers for the convenience of subordinate staff suits equally the convenience of the "snooper". After office hours, keys, if not retained by an official, should be gathered together and locked in a central place, preferably in a safe, or left in the charge of a duty officer.

6. There should be a periodical check of keys of departmental boxes where such are used for the internal circulation of classified documents.

7. Arrangements for the transmission of official documents inside and outside Canada are detailed in Appendix "A". With the exception of material sent by diplomatic bag, all papers, letters, parcels, etc., are normally subject to customs examination in foreign countries. Immunity from examination by customs authorities extends only to diplomatic bags, and does not extend to materials sent by other means even when in the possession of a courier.

Typing and Reproduction Arrangements

8. Loose arrangements for controlling and reproduction of documents and checking the number of carbon copies made can vitiate the most elaborate security precautions. Extra copies are often run off and frequently remain unaccounted for.

9. The danger is difficult to guard against, but it is recommended that departments consider how far the following devices can be adopted in the case of Top Secret and Secret documents:

- (a) special typing pools;
- (b) issue of a given number of sheets to the operators of duplicating machines, all of which are to be returned, or the use of specially coloured paper;
- (c) check on the number of carbons made; and
- (d) special arrangements for the safe custody and destruction of shorthand notebooks.

[6]

Disposal of Classified Waste

10. Classified waste comprises all forms of material bearing security markings, including sheets of carbon paper used in making copies of classified documents, shorthand notebooks and stencil sheets. All classified waste should be torn up into small pieces before it is collected by messenger. All Top Secret and Secret waste should be placed in a separate receptacle and collected under supervision for destruction, where possible, by burning, and where this is not possible, by pulping. Similar arrangements are advocated for the disposal of waste in other categories.

11. Where Secret waste is produced in any volume and adequate facilities for burning it are not available, arrangements should be made for its delivery to a pulping mill under supervision of a responsible officer, who should see personally to its complete destruction.

II. SUPERVISION OF STAFF ENGAGED IN WORK OF A SECRET NATURE

Security Enquiries

(NOTE: The information in paragraphs 12 to 14, inclusive, is confidential and should not be reproduced in any departmental instruction.)

12. It is recognized that, in the public interest, it is sometimes necessary to enquire into the antecedents of prospective and present employees of departments and agencies of government to determine their suitability from the point of view of security.

13. Under the authority of the Civil Service Act the Commission is required to satisfy itself as to the character and habits of persons appointed by it to government employment. These provisions do not, however, apply to all employees of government departments or agencies nor do they relieve departments of their responsibility for satisfying themselves as to the suitability from a security standpoint of the persons in their employ.

14. The government have, therefore, approved a broad policy to cover security enquiries generally and have authorized the Security Panel to devise appropriate procedures designed to achieve some measure of uniformity with regard to these matters.

Administration of Oaths; Declarations Under the Official Secrets Act

15. Under the provisions of the Civil Service Act permanent employees are required to take the Oath of Allegiance, Oath

[7]

004349

AGC-1012_0005

of Office and, in some cases, the Oath of Secrecy. The portion of this Act and specimen forms of the Oaths are given in Appendix "B".

16. The question of whether or not temporary employees and those who are not under the jurisdiction of the Civil Service Commission should make similar attestations is a matter for each department or agency to decide. Arrangements may be made departmentally or with the office of the Clerk of the Privy Council.

17. In addition to the administration of the Oaths, new entrants should read and, if necessary, have explained to them the relevant sections of the Official Secrets Act and they should sign a certificate that they understand its significance.

18. These matters should not be taken care of in a routine or casual manner but the departmental security officer should insure that the implications of the procedure and the vital necessity of living up to the undertaking are explained to the employee. This practice is well worth while and the opportunity of impressing the individual with the need of being security-minded should not be lost.

19. For record purposes a copy of the certificate that the employee understands the significance of the Official Secrets Act should be placed on the individual's file; also an extract from the notification of the Clerk of the Privy Council or other authority for the administration of oaths that the employee has been duly sworn.

Security Training

20. Security regulations and procedure are normally 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.

21. 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 them is their personal responsibility and that the security of the department as a whole is only as good as the security of each member.

22. It is a useful practice to circulate departmental security regulations periodically to all members of the staff in order that the regulations may be kept freshly in mind. It is also useful to conduct lectures from time to time on the various security subjects. Security training films may also be made available through the Department of National Defence.

[8]

I. PHYSICAL SECURITY OF BUILDINGS

Guards

23. By authority of the Governor in Council (see Appendix "C") the responsibility for the protection of departmental buildings is placed upon the Commissioner of the Royal Canadian Mounted Police, subject, in the case of Ottawa buildings, to the concurrence of the Department of Public Works. This arrangement does not apply to buildings occupied by the Department of National Defence, except as may be agreed between this department and the Commissioner, R.C.M.P., and approved by the Treasury Board.

24. The strength of the guard details, the hours of duty and the standing orders under which the guards operate are matters for arrangement between the department concerned and the Commissioner, R.C.M.P. In determining the strength, position and duties of guard details, departmental requirements will vary. The objective must be a guard that meets security requirements but does not unduly hamper the free movement of the staff and visitors. The duties performed by guards must be looked upon as merely one part of the whole security plan and the fact that guards are employed, under the Order-in-Council mentioned, does not remove the primary responsibility for security from individual departments. It is important that departments realize this and ensure that overall arrangements are both adequate and co-ordinated.

Visitors

25. The method of control of visitors to departmental buildings will be influenced by the following factors which should be taken into consideration when drafting security regulations:

- (a) the number of visitors;
- (b) the type of work performed and the volume of classified material handled by the department; and
- (c) whether or not classified material is dealt with throughout the department or merely in certain sections.

Identification

26. There are various systems for controlling visitors. The following are some of the more common:

- (a) Identification, registration and pass — The guard identifies the visitor, registers his particulars, together with the name of the official he is visiting, issues a pass and directs the visitor to the official he wishes to see. The official endorses the pass and the visitor surrenders it to the guard on departure.

[9]

004350

- (b) Identification, registration and escort — The guard identifies the visitor, registers his particulars and has him escorted direct to the official he wishes to see. The official has the visitor escorted back to the exit when his business is completed, and he is checked out by the guard.
- (c) Information office — The guard identifies the visitor and directs him to an information office, where he is interviewed by a departmental official.
- (d) Identification and registration — The guard identifies the visitor, registers his particulars and time of entry, then directs him to the official he wishes to see. He is asked to check out when leaving the building.
- (e) Identification only — The guard merely identifies the visitor, then directs him as requested. Examination of the visitor's identity is limited to persons who are not known to the guard.
- (f) Spot checks only — Visitors enter freely except during periodic intervals fixed at irregular times when all callers are stopped by the guard, their identity checked and their business ascertained. Under this method, the guard may also stop *any* visitor at any time and check his credentials, but normally this step is only taken if the guard's suspicion has been aroused.

27. The method adopted should be considered in relation to other arrangements for internal security, such as the procedure for circulating classified papers, safeguarding secret files and arrangements for supervising offices during quiet periods or during the absence of officials.

28. Quiet hours should be taken as those periods when, under normal conditions, the offices are vacant. It need not include lunch time provided lunch hours are staggered and a skeleton staff is on duty throughout.

Internal Arrangements — Staff

29. In most cases, departments will find it unnecessary to have the staff check in and out during working hours, but it is suggested that, unless the department is carrying out a large volume of work in a high security classification, normal vigilance by staff personnel will eliminate any possibility of unwanted persons securing admission by posing as employees. Departments considering it necessary to check staff in and out should include provision for this within their own regulations.

30. It is considered that all departments should require a check in and check out of the staff working during the quiet

[10]

30. Such personnel should be required to produce pass cards. Their particulars should be noted by the guard, together with the times of entry and exit. Some exceptions may be necessary in regard to particular buildings, but these exceptions should be clearly registered at the guard post so that there will be no misunderstanding or errors.

31. Pass cards admit the bearer to his own department only and should be issued by the departmental security officer.

Internal Arrangements — Offices

32. Good physical security within the offices of a department depend chiefly on the enforcement of appropriate departmental instructions designed to protect classified information. Here, again, any system of office security devised must be governed to some extent by local conditions. It should be the duty of the departmental security officer to ensure that instructions are adequate and that a high standard of office security is maintained through the enforcement of these instructions.

33. The best protection will be gained by locking papers in safes and cabinets when not in use, and particularly during quiet hours. The use of filing cabinets will not, however, give any protection if keys are left about or if the same key can be used to open different cabinets. It should be borne in mind that the development of photography now permits papers to be photographed with a minimum of equipment.

34. Casual workmen should be supervised when working in rooms where access can be gained to official documents.

IV. TELEPHONE SECURITY

Internal Telephones

35. The risk of leakage of conversations between persons using the government exchange in Ottawa arises from casual interception by cross-connection and the possibility of telephone operators and engineers overhearing conversations in the performance of their duties. Many telephones have extensions in other rooms. The possibility should be borne in mind of the second instrument being in the hands of some unauthorized person. The possibility of planned interception on lines in the government exchange and other telephone lines within Canada, while unlikely, cannot be ruled out.

36. "Scrambler" telephones, while not generally in use in government departments, afford only limited security against the expert and, at best, they should be regarded only as a device that will defeat casual eavesdropping.

37. The rule, therefore, is that the telephone should not be used for Top Secret or Secret conversations, except where the

[11]

004351

AGC-1012_0007

need for speed is held to overrule the residual risk of e.g. There is less objection to the transmission of Confidential and Restricted information by telephone, but even so, every effort should be made to render the conversation as unintelligible as possible to the uninitiated.

External Telephones — General

38. It must be assumed that telephone conversations with our missions and representatives outside Canada and all telephone conversations between official premises in countries outside Canada will be monitored. The danger of interception extends equally to intervening countries through which telephone lines pass. It follows, therefore, that no material which it is desired to keep from a foreign government should be transmitted by telephone in countries outside Canada.

External Telephones — Radio

39. Experience during the war has shown that all radio-telephone conversations should be regarded as monitored in any country where the radio signal can be received. Conversations should be limited to subjects of an unclassified nature except where it is possible to deal with matters by reference to documents, copies of which are before both parties, or by any other means, in such a manner that no information is given away by inference. Where calls are prefaced or confirmed by a cypher telegram for this purpose, the telegram should always be sent in a one time cypher. It should be borne in mind that, if code words are used as a device for hiding the meaning of conversations, the use of the same code word in a series of conversations may permit the determination of the meaning of the conversations from a close study of the contexts.

40. It is a desirable practice, from a security point of view, to limit the use of radio-telephone facilities to named officials, and to require other officials who need to make calls to be sponsored by a senior official specially designated. This practice has the advantage of ensuring that the use of radio-telephone is limited to persons practiced in the security technique involved. The number of calls by other officials can thus be kept to a minimum.

V. CYPHER SECURITY

41. This section is intended primarily to apply to departments which do not possess their own cypher offices and which do not frequently have occasion to initiate cypher messages. It does not supersede in any way more detailed instructions that may have been issued by cypher-holding departments.

[12]

42. Cypher security is attained when no unauthorized person is able to gain knowledge of Canadian governmental messages transmitted in cypher.

43. It is essential that Canadian government cypher traffic be not compromised. Complete security for our traffic can and must be maintained. This cannot, however, be achieved by cypher staffs alone; the co-operation of all who originate and receive copies of cypher telegrams is essential.

44. Departments which possess their own cypher offices are in a position to issue such instructions as are necessary to achieve this co-operation from members of their own staffs, but it is equally important that guidance should also be available to all who originate and receive cypher telegrams through the facilities of another department. Precautions should extend equally to copies of telegrams forwarded from one department to another for information.

Security Markings on Messages

45. It is the duty of originators in every case to mark their drafts with the appropriate security classification. This is important as it will influence the cypher staff in their choice of the cypher to be used and will guide the recipient in his handling of the document.

Cypher, Code or Plain Language

46. It is also the duty of the originator to indicate whether his message is to go in cypher, code or plain language.

47. A message transmitted in cypher has security so long as the cypher is properly used by all concerned.

48. A message transmitted in code has no security. It should be regarded as being secure only against casual viewing by those who handle it in transit or by other unauthorized eyes. Generally speaking, its use should merely be regarded as a means of reducing the cost of a plain language message, and not as a measure of security.

49. Messages transmitted in plain language, either by cable or wireless, will, of course, have no security whatsoever.

Marking of Messages by Method of Transmission

50. Messages which are classified at Top Secret or Secret should invariably be marked for despatch in cypher. When a message has a classification lower than Secret, the originator will state whether he wishes the message to be transmitted in cypher or code.

51. The following principles must, however, be observed at all times:

[13]

004352

AGC-1012_0008

- (a) messages received in cypher (with the exception of one time cypher — short title O.T.P.) must be transmitted in cypher;
- (b) messages drafted with a view to publication in whole or in part, or messages containing material which has been or may be published, and the contents of which at the time of despatch it is desired to keep from the knowledge of unauthorized persons must be transmitted in one time cypher and marked "cypher O.T.P." Examples of such messages are:
 - (i) texts of press statements to be released on completion of intergovernmental negotiations, which are confidential until agreement is reached;
 - (ii) draft texts of treaties which have not yet been completed; greeting telegrams which are not considered suitable for publication until after they have been received by the addressee; texts of radio announcements which it is desired to release only at a given date or time.

It is extremely important that the above rule be followed since the cypher staff despatching a message is not always in a position to know whether the contents have been published in whole or in part.

The originator should therefore consider with the greatest care whether the text or part of the text has been or may later be published. If it has been, may be or will be, he must mark it "cypher O.T.P."

- (c) originators who require to quote verbatim from or to repeat to another addressee a cypher telegram which is not marked "O.T.P." or which bears a warning against distribution without paraphrase should mark the new telegram for despatch in "cypher O.T.P."

Multiple Address Messages

52. The originator should consider most carefully exactly to whom he wishes a telegram to be addressed and repeated, and avoid sending it in the first place to one or more addressees and deciding later to send it to others. If it happens that this must be done, he should not, in any circumstances, merely send to the cypher office a copy of the original telegram re-addressed. He should indicate that the message has already been transmitted in order that the cypher office may take such action as security requires.

53. When more than one cypher office is to be employed for the transmission of multiple address messages, each copy

[14]

be marked for despatch in "cypher O.T.P." Such messages should never be marked for despatch in code.

Plain Language or Literal Texts

54. The plain language text of any telegram transmitted in cypher O.T.P. will either be so marked or will not bear a warning against distribution without paraphrasing. The treatment of such messages need not at any stage be affected by considerations of cypher security. If, however, the plain language text of any telegram *does* bear a warning against distribution without paraphrasing, cypher security requires two precautions to be applied irrespective of the security classification of the text. One governs current and the other future handling of the document.

55. The words of the warning must be complied with strictly. If it is necessary to communicate the text in any way to persons who are not in the employment of departments or agencies of the government, it must be thoroughly paraphrased and no mention must be made that the source of information is a cypher telegram. If an originator or a recipient has verbatim copies made of such a telegram, he must ensure that a warning to the following effect is included. "This message must be paraphrased if it is to be communicated to persons outside of the Canadian government service."

56. The plain language text of any telegram not sent in O.T.P. and which bears a warning must for all time be treated as a Secret document. In due course, the subject matter may cease to require any protection, but since it is the verbatim text of a non-O.T.P. cypher message, it must always be treated as a Secret document.

[15]

004353

APPENDIX "A"
SECURITY MEASURES IN RELATION
TO DOCUMENTS

(Revision of Security Panel Administrative
Memorandum of September 4th, 1946)

CLASSIFICATION OF DOCUMENTS

1. Official documents requiring classification will be examined and classified under one of the following categories:

Top Secret

Secret

Confidential

Restricted

2. Classified documents in addition to letters, memoranda, reports, etc., include undestroyed rough copies, stencils and carbon papers; stenographers' note books, photographs and such like.

DEFINITIONS

Top Secret

3. Certain secret documents, information and material, the security aspect of which is paramount, and whose unauthorized disclosure would cause exceptionally grave damage to the nation. The following are examples of subjects falling within this category:

- (a) Very important political documents dealing with such matters as negotiations for treaties and agreements.
- (b) Documents containing plans or details of schemes for the defence of vital strategic areas, including plans or particulars of major operations.
- (c) Critical information of new and important munitions of war, including major scientific and technical developments.
- (d) Important particulars of cryptography and cryptanalysis.
- (e) Minutes or records of discussions of Cabinet or Cabinet Committees.

Secret

4. Documents, information or material, the unauthorized disclosure of which would endanger national security, cause serious injury to the interests or prestige of the nation, or any government activity thereof, or would be of great advantage to a foreign nation. The following are examples of subjects falling within this category:

[16]

- (a) Directives to Canadian representatives conducting important negotiations with foreign powers other than directives which would fall within the Top Secret category.
- (b) Documents containing defence plans or details of schemes for the defence of areas other than vital strategic areas, including plans or particulars of operations connected with them.
- (c) Scientific discoveries of importance to defence measures which do not fall within the Top Secret category.
- (d) Important improvements of existing munitions of war until accepted for general service use, and instructions concerning their use.
- (e) Important government plans — such as, new taxation or trade proposals, new schemes of rationing or other controls.
- (f) Knowledge of strategic importance, the value of which depends upon its possession not being generally known.
- (g) Information on the supply of vital strategic materials.

Confidential

5. Documents, information or material, the unauthorized disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, any government activity, or individual, or would cause administrative embarrassment, or difficulty, or be of advantage to a foreign nation. The following are examples of subjects falling under this category:

- (a) Matters, investigations and documents of a personal and disciplinary nature, the knowledge of which it is desirable to safeguard for administrative reasons.
- (b) Routine intelligence reports.
- (c) Certain documents and manuals of a technical nature.

Restricted

6. Documents, information or material (other than Top Secret, Secret or Confidential) which should not be published or communicated to anyone except for official purposes.

GENERAL PRINCIPLES

7. Classified material is to be entrusted only to those individuals whose official duties require such knowledge or possession. It is the responsibility of the person having custody of such material to ensure that all security precautions are taken to guard this material at all times.

[17]

004354

8. Each document will be classified on its merits, by reference to its contents and their implications and not by reference 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. A reference to a classified document will bear the same classification as the original 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.

9. A document does not normally maintain the same degree of secrecy after a lapse of time. It is important, therefore, to keep the classification of a document under constant review and to downgrade it whenever the necessity for continued protection has ceased. The responsible Deputy Minister will designate a senior official or officials who will be responsible for downgrading classified documents subject to special instructions which may be issued from time to time by the originator or a superior authority. No classified document will be downgraded without reference to the originating authority if there is any doubt as to the wisdom of downgrading it. No Top Secret document which originates with United Kingdom or United States authorities will be downgraded without the consent of the originator.

CUSTODY OF CLASSIFIED DOCUMENTS

Top Secret and Secret

10. Documents will be kept when possible in safes or vaults. When these are not available, steel cabinets may be used, but they should not be accessible to unauthorized persons and keys should be kept by a responsible official.

11. All copies of a Top Secret document should be numbered and a register of recipients kept.

Confidential

12. Documents will be kept in containers which are kept locked and access to them will be open only to officials and confidential clerks.

Restricted

13. Documents will be kept in locked containers.

INTERNAL AND INTER-DEPARTMENTAL CIRCULATION

Top Secret and Secret

14. Transmission within a building is permitted by hand of an official or messenger. If by hand of any official it is advis-

[18]

14. Documents should be carried in a sealed envelope or cover. If by messenger, locked boxes or sealed envelopes will be used.

15. In transmission from one building to another, whether by hand of an official or messenger, documents will be carried either in a locked box or in a double sealed envelope. The inner envelope will be wax sealed, bear the security marking and the inscription "To be opened only by the addressee". The outer envelope will bear the address and will in *no circumstances* bear the security marking.

16. It is mandatory that transmission of Top Secret documents be covered by a receipt system regardless of the method used. Boxes and envelopes will be opened only by the addressee or his authorized representative.

Confidential and Restricted

17. Documents may be carried by hand of messenger or official from one building to another provided they are carried in a locked box or single sealed envelope bearing the security marking.

TRANSMISSION WITHIN CANADA

Top Secret and Secret

18. Documents will be carried from one point in Canada to another either by hand of courier or transmitted by Registered Mail.

If by hand of courier documents will be carried either:

- (a) in a locked box, the key of which will in no circumstances be in the possession of a messenger or official not entitled to know the contents of the document; or
- (b) in a double sealed envelope. The inner envelope will be wax sealed with an official stamp, bear the security marking and the inscription "To be opened only by the addressee". The outer envelope will bear the mailing address of the addressee and will in no circumstances bear the security marking.

If transmission is by Registered Mail it is mandatory that Top Secret and Secret documents at no time leave the territorial limits of Canada. (For the transmission of Secret documents to Newfoundland, see paragraph 23.)

19. Top Secret and Secret documents will be covered by receipt regardless of the method of transmission.

20. When Registered Mail is used for transmission of Top Secret documents, departments are advised to make special arrangements with the Post Office Department for collection of the mail by the addressee or his designated representative.

[19]

004355

Confidential and Restricted

21. Material not sent by Registered Mail will be transmitted by approved official means.

TRANSMISSION OUTSIDE CANADA

22. The Diplomatic Bag of the Department of External Affairs or its missions abroad will be used for the transmission of the following categories of classified documents:

- (a) all Top Secret documents; and
- (b) all classified documents despatched to and from or through territories other than the British Commonwealth or the U.S.A.

23. Bags made up by departments of government other than External Affairs may be used for the transmission of Secret, Confidential and Restricted documents to and from the United Kingdom, other British territories and countries of the British Commonwealth and the U.S.A. *provided* they are carried by couriers and do not pass through another country.

24. Registered Mail may be used providing it does not pass through countries other than those named below, for:

- (a) Secret, Confidential and Restricted documents transmitted to and from Canada on the one hand and British territories and countries of the British Commonwealth on the other;
- (b) Confidential and Restricted documents transmitted to and from Canada and the U.S.A.

It is forbidden to use Registered Mail for the transmission of Top Secret and Secret documents to and from the U.S.A. Exceptions in the case of Secret documents only may be made with the specific authority of a Deputy Minister.

APPENDIX "B"

**REGULATIONS CONCERNING
THE OATH OF ALLEGIANCE, OATH OF OFFICE
AND OATH OF SECRECY**

(Reference Civil Service Act 1918, Section 43)

Every deputy head, officer, clerk and employee permanently employed in the Civil Service, before any salary is paid him, shall take and subscribe the Oath of Allegiance and also the oath contained in Schedule "A" to this Act, or such other oath as is provided by any other Act, in that behalf.

In the case of the Clerk of the Privy Council, and all officers, clerks and employees under him, and in the case of any officer, clerk or employee of whom the Governor in Council requires the same, there shall be added to the oath at the asterisks, in the form of the oath in the said Schedule "A", the words contained in Schedule "B" to this Act.

The Clerk of the Privy Council shall take and subscribe the said oaths before the Governor General or some one appointed by him to administer the same.

In the case of persons residing or coming to reside at the City of Ottawa, the oaths shall be taken and subscribed before the Clerk of the Privy Council.

In other cases the oaths may be taken and subscribed before a justice of the peace or other proper authority, who shall forward the same to the Clerk of the Privy Council.

The Clerk of the Privy Council shall keep a register of all such oaths.

Specimen copies of the Oath, of Allegiance; the Oath of Office and Secrecy; and a Declaration regarding the Official Secrets Act are shown hereunder.

Oath of Allegiance

I.....do swear that I will be faithful and bear true allegiance to His Majesty King George the Sixth, His Heirs and Successors according to the law. So help me God.

Oath of Office and Secrecy

I.....solemnly and sincerely swear that I will faithfully and honestly fulfil the duties which devolve upon me as.....and that I will not without due authority on that behalf disclose or make known any matter or thing which comes to my knowledge by reason of my employment as..... So help me God.

Specimen Declaration Regarding Official Secrets Act

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 unauthorized disclosure of information gained by me as a result of my employment to any person, 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 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.....

**APPENDIX "C"
GUARDING AND SECURITY OF DEPARTMENTAL BUILDINGS**

(Reference Order-in-Council P.C. 178/2502 of June 19th, 1946)

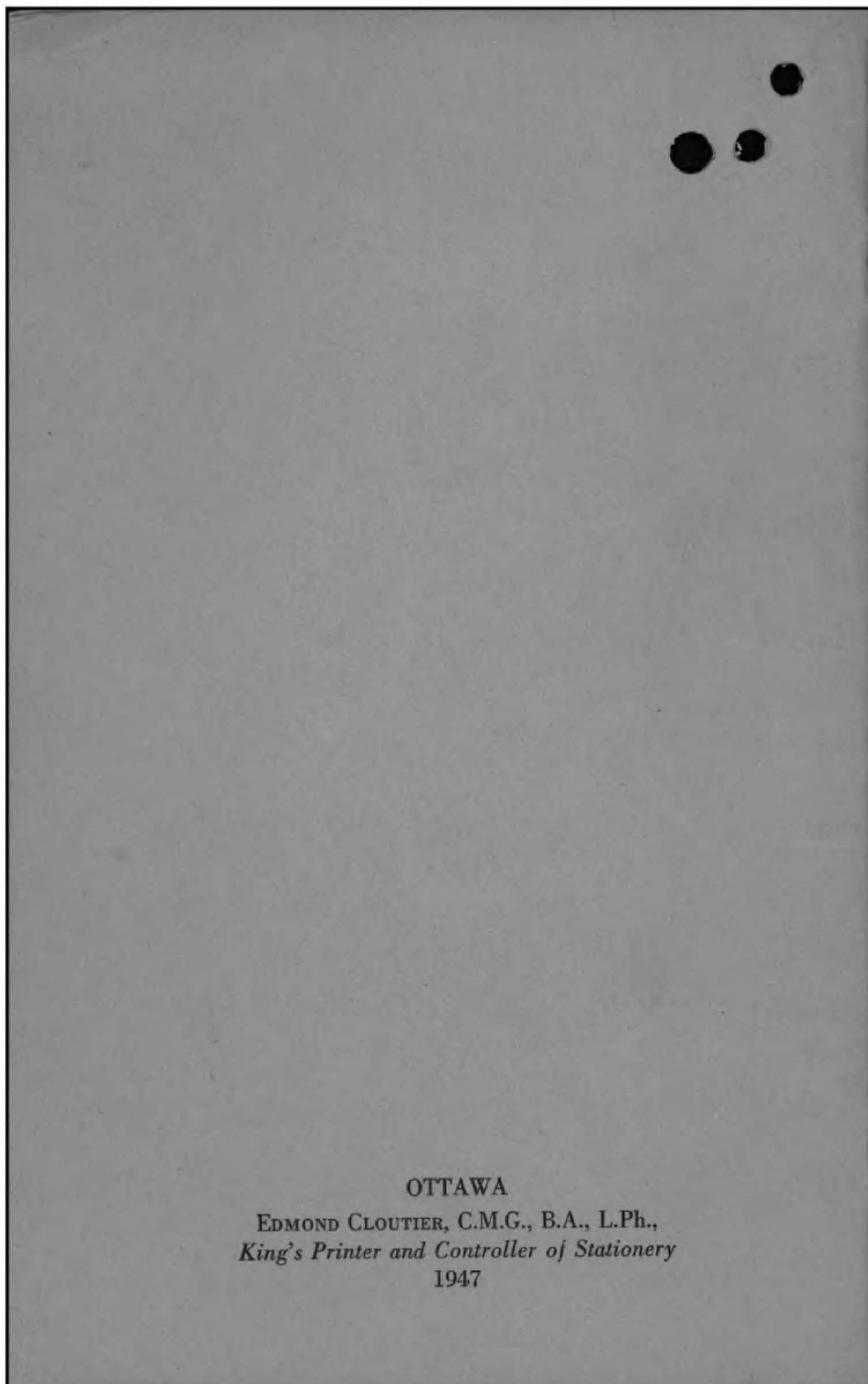
Royal Canadian Mounted Police

The Board recommend that Order-in-Council of February 16th, 1874, P.C. 81, subjecting the Police Force detailed for the protection, care and custody of departmental buildings and adjacent grounds at Ottawa, to the control of the Department of Public Works, be cancelled.

The Board further recommend that the following regulations be approved concerning the guarding and security of departmental buildings and property of the government of Canada:

- (i) The Commissioner of the Royal Canadian Mounted Police shall be responsible for the protection and security of departmental buildings and property of the government of Canada and shall determine the kind and amount of protection which shall be afforded, subject in Ottawa to the concurrence of the Department of Public Works.
- (ii) Departments of government requiring protective facilities shall apply to the Commissioner of the Royal Canadian Mounted Police who shall make such survey as may be necessary to the physical protection of the buildings and property in respect of which the application is made.
- (iii) In the event of a department not being in agreement with the Commissioner of the Royal Canadian Mounted Police as to the protective measures required, the details shall be reported to the Treasury Board and their decision shall be final.
- (iv) The Commissioner of the Royal Canadian Mounted Police shall continue supervision of fire protection to government buildings at Ottawa and report thereon to the Department of Public Works.
- (v) The Commissioner of the Royal Canadian Mounted Police may employ the services of the Corps of Commisaires for guard duty, subject to approval of the Treasury Board.
- (vi) The Commissioner of the Royal Canadian Mounted Police shall submit a report to the Treasury Board as soon as possible after these regulations become effective as to the reduction in Special Constables employed on guard duties.

- (vii) The cost of protective facilities in Ottawa shall be charge to the Appropriation for the Royal Canadian Mounted Police; the cost of such facilities outside Ottawa shall be charged, in the fiscal year 1946-47, in accordance with the provision made in Estimates, and thereafter as may be determined by the Treasury Board.
- (viii) These regulations shall not apply to the Department of National Defence, Department of National Defence for Naval Services and Department of National Defence for Air, except as may be agreed upon between the departments and the Commissioner and approved by the Treasury Board; in any case, the Commissioner shall undertake a review with the said three departments and recommendations shall be made to the Treasury Board not later than July 31st, 1946, with respect to permanent arrangements concerning these departments.



OTTAWA
EDMOND CLOUTIER, C.M.G., B.A., L.Ph.,
King's Printer and Controller of Stationery
1947

004359

AGC-1012_0015