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

December, 1975

P Pfile
S-1-3(a)
(Filed Separately)

DRAFT

PROPERTY OF
PRIVY COUNCIL OFFICE
REGISTRY
Cet ouvrage appartient
a la section de dassement du
BUREAU DU CONSEIL PRIVÉ

HANDBOOK

FOR

DEPARTMENTAL SECURITY OFFICERS

CONFIDENTIAL

AGC-1479_0001

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

RECORD OF AMENDMENTS

Identification of AL		Date Entered	Signature
AL No.	Date		

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

CONFIDENTIAL

A HANDBOOK FOR USE BY DEPARTMENTAL SECURITY OFFICERS

To be approved by the Security Advisory Committee

To be issued by the Security Advisory Committee, 1975

CONFIDENTIAL

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

TABLE OF CONTENTS

CHAPTER	SUBJECT MATTER	ARTICLE
	PREFACE	
	DEFINITIONS	
1.	INTRODUCTION	
	General	101
	Responsibility for Security	102
	Principles of Security	103
2.	SECURITY OF INFORMATION	
	General	201
	Classification Guide	202
	Warning Terms	203
	NATO Security Classification	204
	Extracts	205
	Classification	206
	Under Classification	207
	Over Classification	208
	Preparation and Transmission of Information	209
	Telephone Security	210
	Custody	211

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

Office Custody 212

Custody Outside Work Area 213

In Public Places 214

Careless Talk 215

Entrusting to Persons Outside the Service 216

Loss or Compromise of Classified Information 217

Storage 218

Destruction 219

3. SECURITY OF PERSONNEL

General 301

Clearance Procedures 302

Fingerprints 303

Minimum Standards for Personnel Security Clearance 304

Responsibility for Granting Clearances 305

Investigation Results 306

Security Clearance - Serving Employees 307

Doubtful Clearances 308

Recommendation for Dismissal 309

Quarterly Report to Security Secretariat 310

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

Security Clearance Certification 311

Security Checks - Persons Employed in Defence Industry 312

Security Records - Transferability 313

Security Records - Disposal When Adverse and No Longer Required 314

Personal Behaviour and Social Contact 315

Security Breaches 316

4. PHYSICAL SECURITY

General 401

Physical Security Safeguards 402

Determination of Physical Security Measures 403

Security in Depth 404

Access to Sensitive Areas 405

Security Containers 406

Minimum Storage Requirements 407

Combination Locks 408

Other Locks 409

Service and Maintenance of Approved Security Containers 410

Other Physical Security Equipment 411

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

5. TECHNICAL SECURITY

Communications - Electronic Security (COMSEC)	501
Protection Policy	502
Approved Circuits	503
Unclassified Information	504
Telephones	505
Fallibility of Other Telecommunications Methods	506
Electronic Data Processing (EDP)	507
Electronic Security	508
National COMSEC Agency	509
Planning and Consultation	510
References	511

6. BOMB THREATS

General	601
Organization and Functions of Emergency Organization	602
Responsible Building Authority - Duties	603
Elements of the Departmental Directive	604
Evaluation of Threat	605
Minimizing the Threat	606
Telephone Threats	607
Emergency Contingency Planning	608

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

	Searches	609
	Action on Discovery of Suspicious Object	610
	Evacuation	611
	Security Measures	612
	Coordination	613
7.	MAIL BOMBS	
	General	701
	Mechanically Initiated Letter Bombs	702
	Electrically Initiated Letter Bombs	703
	Soft and Hardcover Book Bombs	704
	Preventive/Protective Measures	705
	Detection	706
	Action to be Taken on Discovery of a Suspect Device	707
	Action to Avoid on Discovery of a Suspect Device	708
8.	ILLEGAL OCCUPATION OF GOVERNMENT BUILDINGS	
	General	801
	Dissident People	802
	Buildings	803
	Protection of Information	804
	Legal Responsibility and Liabilities	805
	Assistance From Police Authorities	806

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

9. FIRST AID

General	901
Objectives and Principles of First Aid	902
General Rules of First Aid	903
Wounds	904
Fractures	905
Burns	906
Artificial Respiration	907

10. VEHICLE PARKING

General	1001
Principles	1002
Parking Methods	1003
Parking Space	1004
Layout of Car Parks	1005

11. PROTECTION OF PERSONAL PROPERTY

General	1101
Responsibility	1102
Property Protection Suggestions	1103
Prevention of Theft	1104

12. FIRE PREVENTION

General	1201
Safety in Case of Fire Emergency	1202
Fire Prevention Educational Material	1203

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

Fire Safety in Offices 1204

Fire Extinguishers 1305

13. SECURITY EDUCATION

General 1301

Objects of Security Education 1302

Methods of Security Education 1303

Visual Aids 1304

Security Regulations 1305

Breaches of Security 1306

ANNEXES

A. Suggested Reading Material

B. Certificate of Destruction

C. Minimum Security Means for Transmission of Classified Matter

D. Official Secrets Act

E. Storage of Classified Materials - Approved Container

F. PSC Regional Offices - Fingerprint Service

G. Security Clearance Questionnaire

H. Security Clearance Certificate

J. Scheduled Countries

K. Security Equipment Guide

L. Combination Lock Operating Instructions

M. Action In Event of Lock-out on Fixed or Built-in Combination Locks

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

N. Telephone Check List

O. Bomb Threat Questionnaire

P. Cabinet Directive Number 45 - Notices of Motion for the Production of Papers

Q. Cabinet Directive Number 46 - Transfer of Public Records to the Public Archives and Access to Public Records held by the Public Archives and by Departments

R. Fire Prevention Educational Material

S. Characteristics of Hand Fire Extinguishers

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

PREFACE

1. This handbook has been designed as a fundamental guide to security and is intended to be used by Departmental Security Officers and other government employees who have been given security responsibilities, but have not had the benefit of either security training or experience to help them perform their duties.

2. There are available a great many commercially produced publications which cover every aspect of security*. Personnel engaged in security work are advised to read extensively in this field to help improve their understanding of what has become an increasingly complex function of business and management administration. To assist in this respect the reader will find at Annex A a list of suggested reading material.

3. This publication is limited to a general overview of security aspects in their simplest form and deals specifically with government security policy as it affects government employees, and the procedures to be followed in the implementation of that policy. It is produced in loose leaf form to facilitate the insertion of amendments from time to time, and users are invited to submit suggestions and ideas for its improvement.

4. Departmental Security Officers should convey to all personnel in their respective departments the principles and policies stated herein, except the detailed information relating to personnel security clearance procedures.

---

*Manufacturers' advertisements may be misleading. Potential purchasers of security equipment should first discuss their security equipment requirements with RCM Police Security Equipment Section and Supply and Services Canada.

AGC-1479_0012

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

INTRODUCTION

101. General

1. Though the RCMP is the main federal operational and investigative body in the field of security, deputy ministers and heads of agencies are responsible for the implementation and administration of security policies within their respective departments and agencies. The RCMP will advise and assist departments and agencies on the implementation of directives, regulations and instructions pertaining to security.

2. The Report of the Royal Commission on Security (1969) noted in its comments on departmental security that standards varied considerably between departments, and that it could be improved. One of the contributory causes for this imbalance was attributed to the lack of recognition given to security, as evidenced by the inadequacy of the strength, calibre, status and training of security staffs. To offset these shortcomings it was recommended that departments should have the services of trained security officers, and that employment in the security field be an accepted part of the process of development of potential senior public servants. In consonance with this, it was made clear that the Departmental Security Officer must be a professional security officer of sufficient seniority to have direct access as required to the deputy minister, and to exert influence over heads of branches or departmental sub-units.

004377

AGC-1479_0013

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

3. Particular stress was placed on the need for security education of not only personnel employed on security tasks, but also of government employees generally.

4. Equally, it was recognized that a need existed by which departments could obtain expert advice and assistance on every aspect of security. This resulted in the formation within the RCM Police of the Directorate of Protective Policing.

5. Early in 1974, a specific statutory authority was issued by the Cabinet in the form of a directive setting out basic principles, allocation of responsibility and arrangements for coordination of physical security measures in the Government service. This Cabinet Directive was issued to replace a number of directives and ad hoc arrangements which had developed gradually after World War II.

6. It is expected that by the time this handbook is taken into use another directive will be issued updating instructions respecting personnel security. Consequently, this handbook covers all those aspects of physical security, security of personnel and security of information required to be known by Departmental Security Officers and their staffs.

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

102. Responsibility for Security

1. With a view to achieving effective, economical and coordinated physical protection of buildings, installations, material and information for which the Government of Canada is responsible, both in Canada and abroad, the basic principles and allocation of specific responsibility is as follows:

a. Deputy Heads of Departments and Agencies

(1) Implementing and administering, within his department or agency, the physical and personnel security clearance policies of the Government of Canada; and

(2) Advising the RCM Police in writing whether or not and to what extent, if any, recommendations made following a security survey have been implemented;

b. Commissioner, RCM Police

(1) Advising deputy heads of departments and agencies (except DND) on the implementation of the physical security policies of the Government of Canada; and

(2) Obtaining assistance of any department or agency for the purpose of carrying out his responsibilities under subsection (1) subject to the approval of that department or agency, if required.

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

c. RCM Police

(1) Conducting security surveys of buildings and vital points (peace and war), as mutually agreed upon by and in cooperation with the departments and agencies concerned, and in accordance with priorities established where necessary by the Security Advisory Committee, at the request of the RCM Police;

(2) Reporting on security surveys and making recommendations thereon to departments and agencies concerned;

(3) Conducting security inspections of buildings referred to in the recommendations of a security survey if, within two years after the date of making recommendations, they have not been advised by the deputy head of a department or agency in accordance with sub-para a.(2);

(4) Maintaining, in relation to such surveys, consultation with DPW and SSC to assist them in carrying out their responsibilities relating to physical security;

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

(5) Coordinating, in cooperation with DEA and DND, technical security inspections that are adequate for the purpose of protecting the Government from technical attacks;

(6) Testing and rating security equipment and material, research and development relating thereto, and quality control in conjunction with SSC;

(7) Reporting the results of security inspections to the departments and agencies concerned and, where necessary, to the SAC; and

(8) Conducting field investigations, records checks and fingerprint checks and providing such other assistance and advice as may be required for personnel security, without limiting in any way the right of the Canadian Forces to conduct field investigations through their own resources, of personnel employed with or on behalf of DND.

d. Supply and Services Canada (SSC)

(1) Ensuring that industrial security measures relating to classified contracts entered into by that Department meet standards developed pursuant to the Cabinet Directive on Physical Security;

(2) Briefing security guard agencies on basic requirements relating to security and emergency procedures, and providing coordination, as necessary, between them and departments and agencies for whom they provide guard personnel;

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

(3) Training of security guards, with appropriate technical and professional assistance from RCM Police and other departments and agencies;

(4) Making contractual arrangements to provide security guards to departments and agencies;

(5) Maintaining a sufficient supply of security equipment for which there is a continuing demand and for contracting for the supply of other approved security equipment upon request; and

(6) Initiating security screening procedures in the case of employees or persons about to be employed in industrial firms and related establishments who require access to classified information.

e. Department of External Affairs (DEA)

(1) Effecting security of its operations at home and abroad, and for the provision of security and security-related resources for that purpose;

(2) Ensuring that the External Affairs Departmental and Post Instructions on Security are applied to members of all departments and agencies at posts abroad; and

(3) Inspecting the control exercised by other departments' and agencies' (except DND) holdings of NATO documents, to ensure that appropriate security is being afforded them in accordance with NATO security regulations.

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

f. Department of National Defence (DND)

(1) Protecting DND building, material and information and operations;

(2) Protecting DND holdings of:

(a) NATO documents in accordance with NATO security regulations, and

(b) foreign military documents in accordance with specific international exchange of information agreements;

(3) Protecting allied military equipments and facilities located on DND property, in accordance with specific international agreements; and

(4) Conducting field investigations, through their own resources, of personnel employed with or on behalf of DND.

g. Department of Public Works (DPW)

(1) Ensuring, with RCM Police advice, that physical security measures are incorporated into all buildings that are being designed, constructed or renovated;

(2) When a building is being designed, establishing committees on which the RCM Police and the departments and agencies concerned are to be represented, to ensure the appropriate coordination of the design for the physical security of the building;

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

(3) Ensuring that physical security is provided for the fabric of all buildings owned or leased by the Government of Canada and may, by agreement with occupant departments and agencies, provide, maintain and supervise additional physical security services for those buildings;

(4) Managing of buildings in its custody and occupied by departments and agencies and by non-government clients;

(5) Providing design services, including engineering, architectural and construction managements with respect to such buildings to meet the needs of its clients;

(6) Providing fire prevention and fire protection services with respect to such buildings;

(7) Installing and maintaining approved security equipment except equipment requiring RCM Police specialists for installation and maintenance; and

(8) Subject to currently approved cost-recovery regulations, and by agreement with the department or agency, and with the advice and assistance of the departmental or agency security officer concerned, providing security guard service for buildings which are not in the custody of DPW.

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

h. Departmental Security Officer

(1) Ensuring the physical security of buildings, premises and installations occupied solely by personnel of his dpeartment or agency;

(2) Protecting information in the custody of his department or agency;

(3) Implementing the personnel security plan in relation to departmental personnel;

(4) Appointing a building security officer, or other officer as approved by the deputy head or head of agency, to assist him in carrying out his security responsibilities when a building is occuped solely by his department or agency, but in which he is not normally employed;

(5) Where a building that is in the custody of DPW is occupied by more than one department or agency, consulting on a regular basis with the property manager (DPW) as to the existing physical security and the future physical security requirements of the building and the occupant; and

(6) Initiating security screening procedures in the case of persons already in the public service, and in the case of persons to be employed under government contract, except those in d.(6).

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

j. Property Manager (DPW)

(1) Subject to any agreement between DPW and an occupant of the building, effecting physical security of the fabric of the building, the external entrances and exits and those other parts thereof that are commonly used by more than one department or agency and commonly available to the public on behalf of more than one department or agency;

(2) Subject to any agreement between DPW and an occupant of the building, providing such other physical security services as may be required due to special circumstances that exist with respect to the building or its occupants;

(3) Where a building that is in the custody of DPW is occupied by more than one department or agency, appointing a committee of occupant departmental or agency security officers or their representatives to advise him as to the existing physical security and the future security requirements of the building and the occupants;

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

(4) Where a building that is in the custody of DPW is occupied by one department or agency, by agreement with that department or agency, and with the advice and assistance of the departmental or agency security officer, providing security guard service applicable to all external entrances and exits of that building or installation or part thereof, and for other security guard service applicable to that building; and

(5) Where a building that is in the custody of DPW is occupied by more than one department or agency, by agreement with such departments and agencies, and with the advice and assistance of the committee referred to at (3) above,

(a) providing security guard service applicable to all entrances and exits, and to all those parts commonly used by more than one department or agency, and to all those parts commonly available to the public, and

(b) providing other security guard service applicable to that building.

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

k. Security Advisory Committee (SAC)

(1) Formulating, for the approval of the Inter-Departmental Committee on Security and Intelligence (ICSI), general standards and procedures for the protection of buildings, material and information for which the Government of Canada is responsible;

(2) Providing assistance and advice to all departments and agencies on the application of such general standards and procedures;

(3) Considering and providing advice to ICSI on proposals for physical security policies and procedures that have been put forward by any of the departments and agencies represented thereon, and on any matters referred to it by the ICSI;

(4) Providing advice and guidance for the resolution of conflicts between the interests of physical security, and departmental and other interests; and

(5) Except for the staffs of government departments or agencies employed as

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

security guards,

(a) developing and maintaining standards of qualifications, security clearances, training and service for security guard services, and

(b) delegating the above responsibilities to a sub-committee of appropriate departmental or agency representatives, including representation from the RCM Police and Supply and Services Canada.

1. Privy Council Office - Security and Intelligence Secretariat

(1) Providing the link between the security community generally and the ICSI, and the Cabinet Committee on Security and Intelligence;

(2) Interpreting and transmitting all directives respecting security issued by ICSI and the Cabinet Committee on Security and Intelligence to the SAC and to the appropriate departments and agencies, and advise on and, where appropriate, coordinate the implementation of the measures referred to in the directives; and

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

(3) Participating in, and providing leadership, as requested and appropriate, in coordinating the formulation of security policy and procedure recommendations to the ICSI and the Cabinet Committee on Security and Intelligence.

m. Security Equipment Advisory Committee (SEAC)

(1) Under the aegis of SAC, and having representatives of RCM Police, SSC, DND, DEA and DPW, setting standards for security equipment and approving security equipment for government use.

2. Each department and agency is, subject to sub-para d.(2) and (3), responsible for the supervision of the service provided to that department or agency by security guards and for taking appropriate measures to ensure that at least minimum standards of service are maintained.

3. The Department of Supply and Services is to be consulted and involved at the requirements definition and procurement stages in relation to the acquisition of guard services and physical security equipment to be supplied by that Department.

4. A department or agency is to ensure that it has clear and effective contingency plans for liaison with its landlord, if any, and with police, fire prevention or other authorities whose

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

assistance may be required for the physical security of the building that it occupies.

5. Notwithstanding paragraph 1 h.(1)(4)(5), j.(1)(2)(3), and paragraph 4, DPW may, by agreement with a department or agency, assume responsibility for the provision of all physical security services in respect of a building occupied by a department or agency.

103. Principles of Security

1. Security measures must apply to all persons who have access to information and material important to the Government of Canada, and to all premises which contain such information and material. These measures must prevent unauthorized persons from gaining access to classified matter and apply safeguards against carelessness or indiscretion on the part of persons who have authorized access. Those persons who are employed by the Government and who might endanger the security of information and material must be detected and excluded from having access.

2. Information which affects Government security must be disseminated only to those persons who have a"need to know" or whose duties require the particular knowledge. All Government employees must be educated to understand the reasons for the importance of observing security measures and of reporting all breaches or suspected breaches of security measures.

AGC-1479_0027

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

SECURITY OF PERSONNEL

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

SECURITY OF PERSONNEL

301. General

1. Before a person is accepted for employment in the government service it is essential that security screening procedures be undertaken to ensure there is no doubt concerning the person's loyalty, reliability and integrity. To effect the screening it is necessary to have enquiries made into the background of employees. For those who are to be given access to classified information the methods by which the enquiries are conducted have been set out in a Cabinet Directive.

2. After the enquiries have been conducted it will be the responsibility of department and agency heads to assess the results and decide the acceptability of an individual to be employed in a position of trust.

3. Persons who by their words or actions consistently show themselves to believe in an ideology or movement which advocates the overthrow of the government by force or any other illegal means should not, when known, be permitted to enter the government service; and those discovered within the service must not be allowed access to classified information.

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

It is also essential that persons be denied access to classified information when it is found they have defects in character which may lead to indiscretion or dishonesty, or which might make them likely subjects of blackmail.

302. Clearance Procedures

1. Government departments and agencies must examine their establishments to determine which positions should be filled by personnel holding clearances. When a need for a specific clearance has been determined the person selected to fill the position should be advised that prior to being appointed a background check will have to be made to establish suitability. The background check will consist of:

a. a security records and fingerprint check for clearance up to SECRET; and

b. a security records and fingerprint check, plus a field inquiry for clearance to TOP SECRET.

2. The individual selected should be asked to complete a Security Clearance Questionnaire with the understanding that the information supplied must be true to the best of his knowledge and that the facts given will be confirmed by investigation. By completing and signing a Security Clearance

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

Questionnaire the subject agrees, in effect, to undergo a security screening. The form of a security clearance questionnaire is at Annex "G".

3. To ensure personnel clearly understand the significance of the security clearance program, departments and agencies should produce locally a form to be attached to the Security Clearance Questionnaire giving the following information:

a. The duties for which you are being considered will bring you in contact with classified information. Before such information is made available to you, you must be subject to security clearance procedures.

b. The Security Clearance Questionnaire form which you are now being asked to complete seeks in strict confidence certain information pertaining to yourself and your immediate relatives. The verification of this information is part of the security clearance programme adopted by the Government of Canada to ensure that its secrets and those secrets entrusted to it by its allies are protected.

c. Clearance procedures are standardized throughout the Canadian government service.

d. A security clearance, once granted, will be

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

upgraded or downgraded in accordance with and individual's changing responsibilities and "need-to-know". Security clearances are reviewed periodically and updated Security Clearance Questionnaires will be required:

(1) when there is a change in the security requirements of the position; and

(2) when there is a change in the data (name changed through marriage, etc.).

e. The clearance programme is impeded when questionnaires are illegible or improperly completed. Therefore all questions should be answered accurately, completely and truthfully. If it is impossible to provide answers to all questions, an explanatory note should be made to indicate the question has not been overlooked.

f. Any information which cannot be accommodated on the form, and which you may feel desirable to disclose, should be provided on a separate sheet of paper, approximatley 8½ x 11",

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

signed and attached to the questionnaire. Completing and signing the SCQ form constitutes your agreement to submit to a security screening.

4. Where possible an unmarked copy of a previously completed Security Clearance Questionnaire should be provided the subject to help in completing the new form.

5. Following the reading of the statement respecting the Questionnaire, the DSO concerned, or his representative, should explain in detail to the subject the security clearance program procedures so that no misunderstanding will exist.

303. Fingerprints

1. In 1954, Cabinet approved a recommendation made by the now defunct Security Panel that all applicants for the public service who were to have access to classified information, and all persons already within the public service who were to be newly given such access, would be required to provide a set of their fingerprints.

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

2. The reason for this decision stemmed from the fact that a security clearance was based on two considerations - a person's loyalty, and a person's general reliability. An important factor in assessing the latter was a knowledge of whether or not the person had a criminal record. Experience had shown that a satisfactory check of a possible criminal record could not be made on a name basis alone, but only by an examination of fingerprints by the fingerprint section of the National Police Service (RCMP). This policy is still in force. Therefore, before a security clearance is granted, two distinct checks must be made by Departmental Security Officers, as follows:

a. Using the Security Clearance Questionnaire a check will be made with the National Security Service against its security records; and

b. Using a standard fingerprint form a check will be made with the National Police Service.

3. Only when the results of both checks are known can a security clearance up to the level of SECRET be considered.

4. The Public Service Commission will normally be responsible for obtaining the fingerprints of new applicants for employment in work of a classified nature in the Public

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

Service. The PSC will forward the prints directly to the National Police Service (RCMP) and advise departments of the results of the check when received. Departments will take no action to hire an individual to do classified work until negative fingerprint and record checks have been received.

5. Federal agencies and departments must clearly specify to the PSC the security classification of its positions at the time of the original requisition to the Commission for appointment.

6. The Public Service Commission provides facilities for taking fingerprints at all its chief offices throughout Canada on behalf of any government department wishing to use the facilities. In locations where the PSC does not provide this service requests may be made to the nearest RCMP detachment. Locations of all PSC Regional Offices providing fingerprint service in Canada are listed at Annex F.

7. Persons already employed by the Public Service who are selected to have access to classified information will be asked by the Departmental or Agency Security Officer to visit the appropriate facility and provide fingerprints on a standard form. The only exception to this concerns those persons who were serving before 1953 and were particularly excluded by Cabinet decision if they were at that time being given access to classified information.

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

8. No sets of fingerprints will be retained by the RCM Police. In the case of applicants for service in government departments or agencies they will be returned under confidential cover to the Public Service Commission. In the case of serving government employees they will be returned to the department, agency, or crown corporation concerned for inclusion on the employee's confidential security file. Should any employee or applicant object to the retention of his fingerprints they may be returned to the employee and a note to this effect placed on his file. Employees who request the return of their fingerprints should be advised that it will be necessary for them to be fingerprinted again when it is necessary to conduct up-dating security clearance procedures.

304. Minimum Standards for Personnel Security Clearance

1. Within the provisions of Cabinet Directive 35, a security assessment and clearance will be based on the following minimum standards:

a. Before a person is employed in a position requiring access to Top Secret information he must be the subject of;

(1) a field investigation,

(2) a records check, and

(3) a fingerprint check.

b. Before a person is employed in a position requiring access to Secret or Confidential information he must be the subject of;

(1) a records check, and

(2) a fingerprint check.

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

2. Where, in the case of a person to have access to Secret information, such checks raise doubt, additional inquiries will be made to resolve it.

305. Responsibility for Granting Clearances

1. The Deputy Head of a department or agency is responsible for granting or withholding a security clearance and assumes a continuing responsibility for employees' access to Top Secret, Secret and Confidential information. In cooperation with departmental officers having management responsibilities, this responsibility should be exercised on his behalf by the Departmental Security Officer with reference to him or his Executive Assistant, as may be required.

2. The process of up-dating or up-grading a security clearance is not designed to inconvenience or embarrass any employee. If it appears necessary on security grounds to recommend against a departmental employee who has access to classified information, the senior Branch and Personnel Officers will be consulted in order to reach a joint agreement respecting the recommendations to be made to the Deputy Minister, or action to be taken.

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

3. Before granting access to classified information, a responsible security officer of the department or agency concerned will make a security determination of eligibility for each individual case investigated.

306. Investigation Results

1. Departments and agencies will be advised of the results of security clearance investigations in the following manner:

a. Top Secret Clearance

The Security Clearance Questionnaire and fingerprint form will be returned showing the results of the checks, and indicating that further inquiries are being conducted. If the preliminary checks against criminal and security records are negative, an interim Secret clearance may be authorized pending receipt of the results of the full field inquiry, if there is an urgent requirement for that level of clearance. Should the results of either check be positive no clearance should be granted until the full inquiry is complete. Where as a result of

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

inquiries, doubt arises about access to highly sensitive material the following course of action may be taken with a view to resolving the doubt:

(1) further specific investigation may be requested of the authorized investigative agency; or

(2) the department or agency may at any time seek the advice of the security secretariat.

b. Secret and Confidential Clearances

The Security Clearance Questionnaire, accompanied by the fingerprint form, will be returned to the dispatching department bearing a stamp indicating either negative or positive findings. If both forms are negative the receiving department may grant a clearance of Confidential or Secret based on the individual's need to know. If the inquiry results in a positive finding, the receiving department will have to make a decision as to the degree of confidence that can be placed in the individual, and whether or not a clearance should be denied.

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

307. Security Clearance - Serving Employees

1. Where a person is already employed in the government service and a doubt is raised respecting his suitability to have access to classified information the departmental security officer must take the action necessary to preserve security. He may also take the course of action referred to in sub-paragraph a. (1) (2) of Investigation Results with a view to resolving the doubt. Should these actions fail to resolve the doubt, or appear to the department to be inexpedient under the circumstances, the assistance of the employee shall be sought in an endeavour to resolve it. A senior officer appointed by the deputy minister shall, after appropriate consultation with the investigative agency or other source of information which raised the doubt, interview the subject and inform him to the fullest extent possible (without compromising important and sensitive sources of information) of the reason for doubt. The employee shall then be given an opportunity to resolve it to the satisfaction of the department.

308. Doubtful Clearances

1. Should none of the courses set out above result in a satisfactory resolution, the responsible department or agency shall withhold a security clearance, take such action as is necessary to preserve security, and consult the securtiy secretariat with a view to determining tentatively:

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

a. whether the subject might safely and usefully be appointed to a less sensitive position in the department or agency, or elsewhere in the government service, in the circumstance;

b. if appointment elsewhere is not possible, whether he should be asked to resign his position in the department or agency, or

c. if he refuses to resign, whether it should be recommended to the minister responsible that he be dismissed from the government service.

309. Recommendation for Dismissal

1. If the deputy head decides that dismissal should be proposed he will so recommend to the Minister responsible, who, if he agrees, will recommend to the Governor in Council that an inquiry be conducted in accordance with the Public Service Security Inquiry Regulations made pursuant to Section 7 (7) of the Financial Administration Act.

310. Quarterly Report to Security Secretariat

1. Departmental Security Officers must forward a report quarterly to the Security Secretariat detailing the number of persons who for any security reasons are removed from eligibility lists by the Public Service Commission, or are for any reason

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

refused access to classified information by departments or agencies. The report will enable the Interdepartmental Committee on Security and Intelligence (ICSI) to review from time to time the number of persons and type of cases involved, and to assess the extent of the security problem in the government service.

2. Figures contained in the report must be broken down into the following categories:

a. Persons dismissed;

b. Persons permitted to resign;

c. Persons transferred to non-sensitive positions;

d. Persons denied access to classified information; and

e. Persons denied employment.

3. Additionally, figures should indicate whether action taken was on ground of disloyalty or unreliability.

4. The number of persons who are no longer given access to classified information solely because of a change in duties or other administrative reason, should not be included.

311. Securtiy Clearance Certification

1. When an individual has been granted a security clearance, a certificate in the form of that at Annex H should be placed on the flyleaf of his security file and should, thereafter, be treated together with his fingerprints, record checks and field reports as an integral part of his permanent security file throughout the remainder of his government service.

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

312. Security Checks - Persons Employed in Defence Industry

1. Supply and Services Canada is the government department responsible for coordinating security checks of persons employed in defence industry (and certain services relating to defence) who may be required to have access to classified information which is the property of the Government of Canada, or for the security of which the government is responsible. Security procedures affecting these persons will be administered by Supply and Services Canada in accordance with a separate directive relating to security in defence industry.

313. Security Records - Transferability

1. Except when they contain adverse information from the National Security Service personnel security records may be transferred freely between departmental security officers.

2. When an employee is transferred from one department to another, the relinquishing department, if it has conducted security clearance procedures must, on request from the Security Officer of the acquiring department, transfer to the acquiring department the Security Clearance Questionnaire, security certificates and the fingerprint form which have been checked by the National Police Services and, except as below, the field investigation report of the National Security Service,

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

if one has been provided.

3. If the file requested contains adverse information from the RCMP Security Service relating to the risk factors described in Annex A to Cabinet Directive 35, the relinquishing department shall return the adverse correspondence to the originator. Though there shall be no transfer of such documents between departments, the Security Officer of the relinquishing department should take the initiative in forewarning and discussing with the acquiring department any adverse information contained on the file prior to returning the documents to the Security Service for review.

4. The relinquishing department should then provide both the Security Service and the acquiring department with an up-to-date security assessment report on the employee concerned.

5. When an employee is loaned or seconded, security clearance documents should not be transferred. The parent department should provide a written statement to the employing department certifying the level of clearance currently authorized. If a higher clearance than the one certified is required, the parent department should take the initiative to upgrade the clearance to the requirements of the employing department.

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

6. The primary purpose of this is to ensure the continuity and relevancy of the security clearance file of an employee, as well as to provide safeguards against the possibility of hasty decisions based on out-dated or incomplete information. The secondary aim is to encourage departments and agencies, through their security staffs, to make and record security assessments on the basis of their personal or acquired knowledge of the employee in terms of his or her loyalty, reliability and integrity within the context of Cabinet Directive 35.

314. Security Records - Disposal When Adverse and No Longer Required

1. All adverse Security Service correspondence which no longer serves a useful purpose should be withdrawn from department and agency security files and returned to the National Security Service. Departments and agencies should undertake to identify and remove from their security record systems all adverse Security Service correspondence on all individuals no longer within the department's sphere of responsibility.

2. Once their security record systems have been cleared of irrelevant adverse files, departments should thereafter be expected to return to the National Security Service all adverse correspondence on:

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

a. unsuccessful applicants for employment in the government service;

b. employees leaving a department or agency on separation, retirement or death;

c. prospective immigrants and other non-immigrant classes, once the prospective immigrant has been granted landed status or denied entry or, in the case of non-immigrants, when the individual departs Canada; and

d. applicants for Canadian citizenship or Certificate of Identity, once the application is approved and the appropriate document issued.

3. Those departments which may have a particular requirement to retain adverse reports for a protracted period of time should inform the National Security Service to this effect and request agreement for the necessary delay.

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

315. Personal Behaviour, Social Contact and Travel

1. Personnel who are engaged on work of a sensitive nature or who have access to classified information must realize that they or their families may be under study by Hostile Intelligence Services (HIS). There are cases on record of persons being targeted by HIS agents even though they are not employed on classified work. Individuals engaged on relatively routine tasks sometimes come under scrutiny of "talent spotters", particularly if they show evidence of some exploitable trait. Evidence in such cases is systematically filed away for use in the event the individual may be eventually promoted or posted into a position considered by the HIS important enough to exploit, or which might make the individual more susceptible to attack by blackmail.

2. Hostile Intelligence Services make deliberate use of social contacts to obtain material for individual dossiers on likely targets. Such contacts may be casual at the outset but it is certain they will not remain so. Government employees must realize that seemingly innocent questions about the identity and function of any other government employees or about their work and circumstances are not necessarily asked out of interest or politeness. Gossip and innuendo concerning the life style, habits and financial position of employees is particularly sought by HIS agents and should be guarded against.

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

3. Social contact with officials and other nationals of countries listed at Annex J should therefore be governed by common sense and a practical awareness of motives. All contacts or approaches should be reported to the departmental security officer.

4. Departmental security officers should brief on the possible security hazards to be encountered, all government employees who have access to classified information and who:

a. travel on business to or through those countries listed at Annex J;

b. travel on leave to or through those countries listed at Annex J; and

c. travel outside those countries listed at Annex J, but on public conveyance facilities of those countries.

316. Security Breaches

1. The responsibility of each member of the government service for protection of classified information cannot be over-emphasized. Even with the best of intentions security

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

breaches can occur. Whether it is the result of the efforts of HIS to penetrate our security defences, or whether it occurs through mistake or negligence, it is the duty of the government employee to report security breaches to the departmental security officer.

2. When a security breach has been reported it is the responsibility of the security officer concerned to conduct an inquiry into the circumstances surrounding it and to make an assessment of its consequences. He should also take immediate corrective action to prevent a continuance or recurrence of the breach.

3. If after investigation of the breach the security officer finds evidence to indicate that unauthorized persons have obtained classified information or have gained access to a restricted area, he should report the incident to his head of department. Departmental heads should ensure that all other organizations affected by the breach are informed as soon as possible.

4. Security breaches involving NATO information should be dealt with in accordance with instructions contained at paragraph 41 (i) of NATO document C-M (55) 15 Final.

5. Full details of any security breach reported or discovered should be recorded and retained on the personal security file of the individual concerned. Major breaches should

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

be reported to the Privy Council Office Security Secretariat.

6. Offenders should be interviewed by the departmental security officer concerned and reminded of their obligation concerning the protection of classified information. Individuals who consistently commit security infractions should be warned that records of their infractions are kept and these, together with assessments of their attitude toward security, will be taken into account in assessing their value to the government service.

7. In extreme cases where wilful disregard of rules has contributed to or caused a major security breach, departmental consideration should be given to the offender's suspension or dismissal. In all such cases the department should seek information respecting previous commission of breaches from the office of the Privy Council Security Secretariat.