Security Policy of the Government of Canada

REVISED
SEPTEMBER 1987

Treasury Board of Canada

Security Policy of the Government of Canada

September 1987

Table of contents

.1 Policy: General

.1.1 Objective and Scope

This policy prescribes a security system that will effectively safeguard classified information and other assets sensitive in the national interest, and protect other sensitive information and sensitive and valuable assets.

It also establishes a job-related screening system.

The policy:

(a) establishes a classification system for information and assets sensitive to the national interest; provides for their declassification and downgrading when sensitivity disappears or diminishes; and prescribes an appropriate security clearance for those whose work involves access to such information and assets;

(b) establishes a designation system for other sensitive information and assets lying outside the national interest and prescribes an enhanced reliability check for those who work with such information and assets;

(c) reaffirms basic protection, reflecting good management practices, for all information and assets and makes a basic reliability check mandatory, with specified exceptions, for all those working for or in the government; and

(d) directs institutions to develop their own security practices and procedures and to assign internal accountability for their management, and makes institutions responsible for detecting breaches and violations of security and applying appropriate countermeasures and sanctions.

In so doing, this policy will prevent the improper classification of information and avoid unnecessary security clearances.

.1.2. Definitions

For the purpose of this policy, the national interest concerns the defence and maintenance of the social, political and economic stability of Canada, and, thereby, the security of the nation. Such information is described in the specific sections of the Access to Information and Privacy Acts as set out in Section .2 below.

Also for purposes of this policy, "other sensitive information" lying outside the national interest refers to information that might be reasonably expected to be exempt under the provisions of the Access to Information Act and the Privacy Act set out in Appendix D.

.1.3 Application

This policy applies to all departments and other institutions and portions of the Public Service of Canada listed in Schedule I, Parts I and II of the Public Service Staff Relations Act, including the Canadian Armed Forces, the Royal Canadian Mounted Police and the Canadian Security Intelligence Service.

Security screening services and certain other institutions that need access to classified information and other assets sensitive to the national interest are also governed by the requirements of this policy that apply to the national interest. Coverage is arranged through agreements between the President of the Treasury Board and the Ministers responsible for these institutions. Agreements shall include a statement of the measures to implement safeguards in the national interest within the institutions concerned. Effective January 1, 1987, only institutions subject to such agreements shall have the access to information, other assets and services described above.

Except as otherwise noted, all appointments, assignments and contracts for goods and services are subject to the provisions of this policy.

.1.4 Authorities and cancellations

This policy is issued under the authority of the Financial Administration Act, by which the Treasury Board may act on all matters relating to administrative and personnel policy in the Public Service of Canada, and of a decision of Cabinet in January, 1986 regarding security measures. Treasury Board minute 802143 applies.

The policy replaces the 1956 Privy Council Office document entitled, "Security of Information in the Public Service of Canada"; Cabinet Directive 35 of 1963, relating to security screening; Chapter 440.8, EDP: Security; and section .6 of Chapter 435, Telecommunications administration, of the Treasury Board Administrative policy manual. It also replaces the policies published in Treasury Board Circulars 1986-26, 1987-10 and 1987-31.

.1.5 Accountability

Deputy heads of departments and heads of agencies (henceforth called deputy heads) have full authority for the administration of all aspects of their institution's security.

They are accountable to the Treasury Board Secretariat to ensure that good security practices are in place. Each shall designate a senior official to coordinate and direct the implementation of the Security Policy.

In screening personnel for reliability and security, deputy heads must,

(a) determine the screening requirements, based on the need for access to information or assets classified in the national interest or access to other sensitive information or sensitive or valuable assets;

(b) decide, after examining the information obtained about an individual, whether any risk attached to his or her appointment or assignment is justifiable, and accept responsibility for the decision; and

(c) provide notice to individuals, as required by the Canadian Security Intelligence Service Act and this policy.

The Treasury Board Secretary is accountable to the Treasury Board and the Security and Intelligence Committee of Cabinet for developing, implementing and interpreting this policy; for coordinating the development of government-wide security standards and advising on their adoption; for monitoring compliance with and evaluating the effectiveness of this security policy; and for reporting on its implementation. This will be done by drawing upon the information systems of institutions, such as internal audit.

Within the Department of National Defence and the Canadian Armed Forces, where the standards developed on the basis of this policy are not effective or practicable in the context of military or national emergency operations, commensurate security may be provided.

.1.6 Roles and responsibilities

.1.6.1 The Privy Council Office is responsible for advising deputy heads on decisions to order a formal investigation of suspected breaches of security, and on decisions to deny security clearances. The Privy Council Office also provides general guidance and advice on substantive decisions to deputy heads, and to the senior officials they designate, and establishes procedures for declassifying confidences of the Queen's Privy Council for Canada and records administered under the Cabinet Papers System. The Privy Council Office also performs certain functions assigned by this policy as they relate to specified Governor-in-Council appointments.

.1.6.2 The Department of the Solicitor General is responsible for providing advice and assistance to the Treasury Board Secretariat in the development of government-wide policy and procedures pursuant to this policy.

.1.6.3 Government-wide and other roles A number of committees and institutions have roles in implementing this policy that affect other departments and agencies. These are set forth in Appendix A.

.2 Classified information and assets

Information shall be classified, protected and declassified or downgraded in accordance with this section. Other assets shall be protected in accordance with article .2.8.

.2.1 Information to be classified

Government institutions shall classify information when its unauthorized disclosure or other compromise by whatever means could reasonably be expected to cause injury to the national interest.

Institutions shall therefore classify information that would probably be exempt from access or excluded under the Access to Information Act (ATIA) or the Privacy Act, as follows:

(a) where compromise could reasonably be expected to be injurious to

- the conduct by the Government of Canada of federal-provincial affairs (s.14, ATIA; s.20, Privacy Act),
- international affairs and defence, including the detection, prevention or suppression of subversive and hostile activities (s.15, ATIA; s.21, Privacy Act), or
- the economic interests of Canada (para.18(a) and 18(d), ATIA);

(b) where the information is obtained or prepared by an investigative body during lawful investigations into activities suspected of being threats to the security of Canada within the meaning of the Canadian Security Intelligence Service Act (sub-para.16(1)(a)(iii) and 16(1)(c), ATIA; sub-para.22(1)(a)(iii) and para.22(1)(b), Privacy Act);

(c) where the information relates to investigative techniques or plans for specific lawful investigations in relation to (b) above (para.16(1)(b), ATIA);

(d) where the information would reveal the identity of a source in relation to the security clearance process (s.23 and para.22(1)(b), Privacy Act, re: the granting, and review and updating of clearances);

(e) where the information contains advice, etc. relating to (a) to (c) above (s.21, ATIA);

(f) where the information relates to (a) to (c) above and its disclosure is prohibited by certain statutory provisions (s.24 and Schedule II, ATIA);

(g) where the records and drafts thereof constitute confidences of the Queen's Privy Council for Canada (as described in s.69, ATIA or s.70, Privacy Act) including Treasury Board Papers (see Appendix I) that contain information relating to (a-c) above;

(h) where records and drafts thereof are administered under the Cabinet Papers System. (See Appendix H).

The legal basis for determining whether information may be classifiable in the national interest is set forth by specific sections of the Access to Information Act and the Privacy Act. Legal interpretation and government policy on the application of these provisions is contained in the Treasury Board Interim Policy Guide: Access to Information Act and the Privacy Act, Parts II and III (TB Circular Letter 1983-35).

No information, other than that exempt or excluded in accordance with the Guide, shall be classified in the national interest. In no case may information be classified in the national interest in order to conceal violations of law, inefficiency or administrative error, to avoid embarrassment, or to restrain competition.

Classified information received from provincial, municipal or regional governments, from governments of other nations or from international organizations of nations or their institutions shall be treated as TOP SECRET, SECRET or CONFIDENTIAL, as applicable, in accordance with agreements or understandings between the parties concerned.

.2.2 Levels of classification in the national interest

*Information shall be classified as:

- TOP SECRET when compromise could reasonably be expected to cause exceptionally grave injury to the national interest;

- SECRET when compromise could reasonably be expected to cause serious injury to the national interest; or

- CONFIDENTIAL when compromise could reasonably be expected to cause injury to the national interest.*

These classifications shall not be used for any purpose other than to classify information in the national interest.

Government institutions shall classify information at the level necessary to safeguard the national interest. Institutions shall develop their own guidelines indicating the necessary classification level for each kind of information. In preparing these guidelines, institutions should carefully balance the possible injury from unauthorized disclosure, destruction, removal, or modification against the cost of safeguarding information at high levels of classification. Guidelines shall be incorporated into the departmental information classification guides prescribed in article .2.3.

While the RESTRICTED designation is not part of the Canadian classification scheme, information so designated, received from NATO countries or OECD sources, must be protected in accordance with agreements or understandings between the parties concerned. The designation RESTRICTED may be assigned to information originating in the Government of Canada only when it relates to information designated RESTRICTED by NATO or OECD sources.

.2.3 Authority to classify information in the national interest

*Information shall be classified in the national interest:

- by employees, only when the classification is governed by a classification guide, approved by the deputy head; or

- by appointed officials, when particular information is not covered by such a guide. Deputy heads must appoint officials in writing.*

Classification guides must reflect this policy, describe the kinds of information to be classified, and indicate the levels of classification to be applied.

Classification guides and lists of appointed officials are to be reviewed annually to ensure that guides are current, explicit and as comprehensive as possible, and that classification authority is still required for the officials appointed.

If an employee needs a classification decision in the absence of an appointed official, the employee may mark the information at the level he or she deems appropriate, provided the decision is confirmed within thirty days by the appointed official concerned.

No authority is needed to classify information that derives from other information already classified in accordance with this policy. Examples include extracts and summaries. This also applies to contractors, who may mark information derived from classified information provided by a government institution.

Institutions must ensure that all employees, contractors and appointed officials engaged in classifying information have a current security clearance that matches the highest level of the information to which they have access.

.2.4 Duration of classification

Information shall be classified only for the period of time it needs protection in the national interest. It shall be declassified or downgraded when such protection is no longer necessary, or is no longer needed at the same level.

.2.5 Marking

Classified information shall be marked or identified at the time it is created or collected, to alert those who use it that it must be safeguarded at the applicable level.

Marking shall include:

- the applicable classification level; and
- the date or event at which declassification or downgrading is to occur, when it is possible to determine this at the time the information is created or collected.

When documents are marked TOP SECRET and SECRET, the classification level shall be indicated on every page. For other media (e.g. EDP data), marking shall be indicated in a manner appropriate to the medium concerned.

When documents are marked CONFIDENTIAL, the classification level shall be shown on the face, at a minimum, and on other pages as well, if deemed necessary by the deputy head.

.2.6 Protective measures

*Government institutions shall safeguard classified information:

- by limiting access to those persons that have a "need to know" in order to perform their duties or tasks and a current security clearance at the appropriate level; and
- by applying the standards approved by Treasury Board covering physical, information technology and personnel security that will safeguard the information at the required level; or
- where applicable, by ensuring, through agreements or understandings, that governments or organizations not subject to this Security Policy also protect that information appropriately, including, where necessary in particular circumstances, federal government security clearances.*

Advice on protective measures and other aspects of this policy is available from the institutions specified in Appendix B.

.2.7 Declassification and downgrading

Government institutions shall declassify information when it no longer needs safeguarding in the national interest and shall downgrade the classification of information when safeguards are no longer needed at the higher level. Declassification and downgrading are to be carried out in accordance with the principles set out in Appendix C (elaborated in government-wide standards). These should, whenever possible, be incorporated into an institution's classification guide.

Confidences of the Queen's Privy Council for Canada that are classified and records that are administered under the Cabinet Paper System remain classified if they have been in existence for less than twenty years. Only in very rare instances will such records be declassified or downgraded before they have been existence for twenty years. After twenty years, these records can be declassified or downgraded pursuant to the principles set out in Appendix C.

.2.8 Assets sensitive in the national interest

Assets, such as materiel and government installations, must have special safeguards when compromise could reasonably be expected to cause injury to the national interest. *Government institutions shall safeguard such assets in accordance with standards approved by Treasury Board.*

.3 Other sensitive information and sensitive or valuable assets

.3.1 Information to be given enhanced protection

Some information that lies outside the national interest, and therefore cannot be classified, is nevertheless sensitive and requires enhanced protection.

Government institutions shall give enhanced protection to information lying outside the national interest if that information is reasonably likely to be exempt or is excluded from access under the provisions of the Access to Information Act or Privacy Act set forth in Appendix D.

The basis for determining whether information requires enhanced protection is set out in the Treasury Board Interim Policy Guide on the Access to Information Act and the Privacy Act, Parts II and III.

The Privacy Act establishes controls on the collection, use and disclosure of personal information in order to protect the privacy of individuals. *Personal information, as defined in Section 3 of the Privacy Act, is a special case and shall be given enhanced protection.* Such information is subject to a mandatory exemption under the Access to Information Act (s.19). A certain amount of sensitive personal information must be protected above the minimum standards when it is transmitted.

"Particularly sensitive personal information" is defined as personal information, the compromise of which could reasonably be expected to cause serious injury. Examples that might qualify are very sensitive medical information, financial information or personal evaluations. *Institutions are required to review their holdings of personal information to determine if, in the opinion of the deputy head, any of it qualifies as particularly sensitive personal information. Special practices and procedures for dealing with it, especially when it is transmitted, are to be established.* Guidance in identifying particularly sensitive personal information is provided in the introduction to the government-wide security standards.

Problems arise when personal information is stored in a format where data on a large number of individuals is involved (eg. microfiche, EDP tapes etc.). Institutions should develop special practices and procedures, in addition to the government-wide security standards, to deal with this type of documentation.

Unclassified information obtained "in confidence" from other governments or organizations, as described in section 13 of the Access to Information Act and section 19 of the Privacy Act, shall be protected in accordance with this section and article .4.6.1, Part II, of the Treasury Board Interim Policy Guide on the Access to Information Act and the Privacy Act. Information is to be marked as received "in confidence", with an indication of the source, before it is distributed to other government institutions. Article .4.6.1 further requires consultation with the originating institution before disclosure.

Enhanced protection is to be given to the sensitive information referred to here by means of the measures set out in article .3.4.

.3.2 Authority to designate other sensitive information

*Information shall be designated as "other sensitive information":

- by employees, only when the information is governed by a designation guide approved by the deputy head; or
- by appointed officials, when particular information is not covered by such a guide. The deputy head must appoint officials in writing.*

Designation guides must reflect this policy and describe the types of information to be designated.

No authority is needed to designate information derived from other information already designated in accordance with this policy. This also applies to contractors, who may mark information derived from designated information provided by a government institution.

.3.3 Marking

Other sensitive information should be marked or otherwise identified at the time it is created or collected, to alert those who use it that it requires enhanced protection.

An institution may not deem it necessary to mark or otherwise identify such information at the time it is created or collected, because those working with it may be especially attuned to the need to give it enhanced protection. Such an approach is permitted.

*Institutions shall, however, mark such information if it is to be disclosed beyond the organizational unit that created or collected it (i.e. section, division, branch or entire institution, as determined

by the deputy head).* Marking is not required when the information is intended for a use which will make it publicly available or when it is routine personal information (eg. a cheque) exchanged with the individual involved or his or her representative.

Proper marking requires the word PROTECTED on the face of all documents concerned or, with respect to other media (e.g. EDP data), in a manner appropriate to the medium. Institutions may choose to add words denoting why information is protected, using the designations listed in Appendix D (e.g. PROTECTED-Business Information). *An exception is Cabinet confidences, which shall be marked only as PROTECTED, with no additional words.*

Government institutions may remove the marking PROTECTED from information when it no longer requires safeguarding as other sensitive information. In removing such markings, the guidelines given in article 2.7 should be adapted.

Confidences of the Queen's Privy Council for Canada that are designated PROTECTED remain protected if they have been in existence for less than twenty years. Only in very rare instances will such records have the marking PROTECTED removed. Once a record has been in existence for more than twenty years, a government institution may remove the marking, in accordance with the principles set out in Appendix C.

.3.4 Protective measures

*Government institutions shall accord enhanced protection to sensitive information that lies outside the national interest and which could reasonably be expected to be exempt from access under the Access to Information Act or the Privacy Act:

- by limiting access to those persons who have a "need to know" in order to perform their duties or tasks, and who have met the requirements of an enhanced reliability check; and

- by applying standards approved by Treasury Board covering physical, information technology, and personnel security; or

- where applicable, by ensuring, through agreements or understandings, that governments or organizations not subject to this Security Policy that share sensitive information also safeguard it.*

.3.5 Sensitive or valuable assets

Assets other than information, such as cash and other negotiable instruments, and equipment and other sensitive or valuable materiel, may merit enhanced protection.

Government institutions shall protect sensitive or valuable assets by limiting access to those persons who require it to perform their duties or tasks and who have met an enhanced reliability check, and by applying the standards for physical security approved by Treasury Board.

.4 Other information and assets

Most government information and other assets fall outside the categories "classified" and "other sensitive information" and sensitive or valuable assets. *However, institutions shall protect all other information and other assets in accordance with records management, EDP, materiel, financial and personnel policies of Treasury Board. Institutions shall limit access to those who require it to perform their duties or tasks.*

.5 Threat and risk assessment

In determining how to safeguard classified and other sensitive information and valuable assets, institutions shall carry out threat and risk assessments.

Once the potential for injury has been determined, additional judgements must be made about the type of threat to which a given asset may be exposed and the likelihood or risk of its occurring. These threat and risk assessments will enable an institution to decide if safeguards above the minimum set out in the government-wide standards should be used. Guidance on conducting threat and risk assessments is provided in the introductory chapter to the security standards.

In making a decision about added safeguards, institutions shall balance the gravity of the potential injury against the effectiveness and costs of the planned protection.

.6 Personnel reliability and security screening

.6.1 Basic reliability checks

A basic reliability check is a condition of appointment to the Public Service and shall be conducted by government institutions for all appointments, assignments (including secondment and interchange) and contracts for service of more than six months' total duration.

For contracts, appointments and assignments to the Public Service of less than six months' total duration, a reliability check is optional. Government institutions must consider the nature of the duties or tasks to be performed and the sensitivity or value of the material to which there will be access, and may choose to conduct a reliability check, eliminating non-essential or impractical elements, depending on the type or length of the assignment, appointment or contract.

A basic reliability check for current federal government employees is at the discretion of the deputy head, as are the elements to be included (see Appendix E).

*Government institutions shall ensure that the following are carried out as part of the basic reliability check:

- verification of personal data;
- verification of educational and professional qualifications or trade certification or accreditation;
- verification of employment data;
- assessment of performance and reliability, by checking with previous employers and identified references;
- name check of criminal records; and
- a check of the Public Service Commission's Central Index of employees released, rejected on probation or dismissed or discharged for cause (see role in Appendix A).*

Key requirements for a basic reliability check are contained in Appendix F.

.6.2 Enhanced reliability check

Government institutions shall conduct an enhanced reliability check when an appointment, assignment, or contract involves, to a significant degree, the care and custody of, or access to, sensitive information or sensitive or valuable assets that are not classified in the national interest. It is a condition of appointment, employment or assignment, as applicable.

In addition to the elements of the basic reliability check, an enhanced reliability check requires:

- a fingerprint check, except for current federal government employees where the deputy head may decide that a criminal records name check will suffice;
- a credit check, when the duties or tasks to be performed, in the opinion of the deputy head, require it; and
- other checks, according to the duties or tasks to be performed. Such checks may, however, be implemented only with the prior approval of the Treasury Board.

Key requirements for an enhanced reliability check are set out in Appendix F, but it is important to bear in mind the qualifiers set out here.

.6.3 Security clearances

*Government institutions shall arrange for the security clearance, at the appropriate level, of all individuals whose duties or tasks REQUIRE access to classified information or other assets sensitive to the national interest OR of those who have access to essential

persons or installations critical to the national interest that, in the opinion of the deputy head, affords regular and consistent access to such information or assets.*

When a security clearance is required, it is a condition of appointment and employment. When required, it is mandatory for individuals on secondment, interchange assignments, SAPP assignments, and acting assignments. When required, it is mandatory for contracts.

There are three (3) levels of security clearance for access to classified information or assets. The relationship of each level to the security classification scheme is as follows:

Level 1 - Confidential
Level 2 - Secret
Level 3 - Top Secret

Deputy heads shall grant or deny a security clearance, taking into account advice from the investigative body and the Departmental Security Officer.

Before denying a security clearance, deputy heads may wish to consult with the Intelligence and Security Coordinator of the Privy Council Office.

The authority to deny, revoke or suspend a security clearance rests with the deputy head and shall not be delegated.

A security clearance must involve, at a minimum, those elements detailed in the chart in Appendix E. Other conditions are set out in Appendix G.

.6.4 Screening positions

All new job descriptions shall be reviewed to determine if the duties or tasks provide access to classified information or assets or to designated information or assets, and therefore require the incumbent to be subject either to security clearance or to enhanced reliability screening.

The requirement for a basic or enhanced reliability check or security clearance shall be noted on TB 330-167 or other similar form presently in use by government institutions.

For current job descriptions, departments shall undertake (as part of their cyclical classification review, whenever a job description is submitted for update, or as directed by the deputy head) a review of each position to identify those that require an enhanced reliability check or security clearance. All positions must have been identified within two (2) years after this policy comes into force.

.6.5 Administrative cancellation

Where an individual no longer requires an enhanced reliability check or security clearance these shall be cancelled. The individual must be informed that the cancellation is solely for administrative reasons and does not reflect on his or her reliability or loyalty. TBS form 330-25 (86/4) "Administrative Cancellation of Enhanced Reliability Check or Security Clearance" shall be used.

.6.6 Periodic update and review

Government institutions are required to update an employee's enhanced reliability check or security clearance at least once every five years, or more frequently, at the discretion of the deputy head.

.6.7 Administrative arrangements

When individuals do not meet the requirements for access to classified or designated information or assets, either as a result of an update or review or because the requirements of his or her position have changed, institutions shall limit or prevent their access to such information and assets. When these individuals are employees, possible arrangements may include reassignment or appointment by the deputy head to a less sensitive position at an equivalent level. Should no such position be available, appointment to a position at a lower level is to be considered. Termination of employment may be considered only in exceptional circumstances and when all other options have been exhausted. In addition, deputy heads are required to consult with the Privy Council Office before recommending to the Governor-in-Council the suspension or dismissal of any person in the interests of security, as provided for in subsection 7(7) of the Financial Administration Act.

.7 Breaches and violations of security

.7.1 Breaches

A breach of security is deemed to have occurred when any classified or designated information or assets have been the subject of unauthorized disclosure or unauthorized access. Without restricting its scope, a breach may include unauthorized disclosure by any person, theft, and loss or exposure in circumstances that make it probable that a breach has taken place.

Possible breaches of security shall be reported immediately to the deputy head. Institutions shall then assess the circumstances to determine whether it is probable that a breach has occurred.

Suspected breaches constituting criminal offences shall be reported to the appropriate law enforcement authority.

Probable unauthorized disclosure of, or unauthorized access to classified information shall be reported immediately to CSIS.

.7.2 Injury assessments

Government institutions shall, within ten (10) working days, conduct an assessment of injury whenever it is probable that a breach of security has occurred.

Injury assessments shall be in writing and shall contain the following:

- identification of the source, date and circumstances of the breach;
- classification or designation of the information or asset in question;
- a description of the information or other asset concerned; and
- a statement and analysis of the injury to the national or other interest that has resulted, or may result.

Whenever a breach of security occurs in an institution that did not originate the information or other assets involved, the originating institution shall be notified and furnished with all particulars, so that an injury assessment may be initiated.

Whenever a breach of security involves the information or other assets of more than one institution, each institution shall advise the other(s) of the circumstances and findings that affect them. Whenever an injury assessment incorporating the work of two or more institutions is needed, the institutions affected shall agree upon who shall be made responsible for the assessment.

.7.3 Reports to deputy heads

*Breaches of security and the findings of all injury assessments shall be reported to deputy heads, along with the following additional particulars:

- interim steps taken to nullify or minimize the effect of the breach (e.g. modification of the information); and
- whether or not a formal investigation of the breach is recommended.*

.7.4 Investigations

The deputy head shall decide if a breach of security is to be investigated. In arriving at such a decision, departments may consult with the Privy Council Office to determine whether a formal investigation is to be undertaken. The deputy head may also wish to consult with the Deputy Commissioner, Operations (Criminal), Royal Canadian Mounted Police. The results of investigations shall be reported to the deputy. Where the breach of security affects other institutions or other governments, they may be involved in the investigation. In any event they shall be apprised of its results.

.7.5 Violations

*A violation of security is any action that contravenes any provision of this policy. Without restricting its generality, a violation is deemed to have occurred when any person:

- fails to classify or designate information in accordance with this policy;

- classifies or designates or continues the classification or designation of information in violation of this policy;

- modifies, retains, destroys or removes classified or designated information or assets without authorization; or

- causes the unauthorized interruption of the flow of classified or designated information.*

Violations shall be reported to the senior official responsible for the operational area concerned. Where appropriate, corrective measures shall be undertaken.

.8 Sanctions and redress

.8.1 Sanctions

Sanctions shall be applied in response to breaches and violations of security when, in the opinion of the deputy head, there has been misconduct or negligence.

Sanctions are administrative, disciplinary or statutory in nature. They can be applied to any action that contravenes this policy. Institutions may obtain advice from their legal advisers on whether statutory sanctions should be contemplated in particular cases.

Deputy heads have the discretion to apply any of the following administrative and disciplinary sanctions, or a combination of these, taking into account the nature of the breach or violation, the past performance of the person concerned in the discharge of security responsibilities, and the surrounding circumstances:

- termination of classification authority;

- removal of security clearance and loss of access to classified information or assets sensitive to the national interest;

- removal of enhanced reliability status and loss of access to designated information and sensitive or valuable assets; and

- the full range of disciplinary sanctions (oral reprimand, written reprimand, suspension with or without pay, discharge).

.8.2 Redress

Redress for disciplinary sanctions, except the removal of security clearances, is available through the relevant provisions of Sections 90 and 91 of the Public Service Staff Relations Act or equivalent procedures for employees not subject to that Act. A person whose security clearance has been removed may have recourse to the formal review process of the Security Intelligence Review Committee, as specified in the Canadian Security Intelligence Service Act.

.8.2.1 Reliability checks

Employees who wish to challenge a negative decision based only on the results of a basic or enhanced reliability check may do so through current grievance procedures. Government institutions, other than the Canadian Armed Forces component of the Department of National Defence, will ensure that such grievances proceed directly to the final level. In addition, the deputy head responsible for the decision is delegated the authority to deal with such grievances and such grievances should be processed to his or her office.

.8.2.2 Security Clearance

The Security Intelligence Review Committee is responsible for the formal review process for redress concerning denial of a security clearance. This review is available to outside candidates, employees and contractors. Where an individual who has been denied a security clearance appeals to the Canadian Human Rights Commission, the Canadian Security Intelligence Service must be informed in order that the Director of the Canadian Security Intelligence Service may determine whether the appropriate Minister should be advised to notify the Canadian Human Rights Commission, as provided for in paragraph 36.1(2) of the Canadian Human Rights Act.

.8.3 Screening review process

While the procedures outlined above are the formal review and redress mechanisms, government institutions are encouraged to establish a "Screening Review Process" to review decisions that affect employees negatively.

.9 Implementation

Implementation should include:

- the naming, by the deputy head, of a senior official to coordinate and direct the implementation of this policy;
- the development of institutional guidelines for the classification and designation of information;
- the development of a security policy and procedures manual consistent with this policy;

- the declassification and downgrading of existing information holdings. This should include, where feasible, declassification of blocks of information;

- the completion of threat and risk assessments;

- the application of government-wide standards and other safeguards;

- a review of all positions to determine if a security clearance or an enhanced reliability check is needed; and

- a review of the institution's security function, including its roles and structure.

.10 Accountability

.10.1 Reporting requirements

The Treasury Board Secretariat monitors compliance with the policy and reports to Treasury Board and to the Cabinet Committee on Security and Intelligence on its application. The first report is due in July, 1988.

In 1987-88, institutions shall undertake an internal review of the application of this policy in their institutions. Deputy heads shall report on the results of the review to the Secretary of the Treasury Board by April 1, 1988. Additional reports may also be required.

Questions will be provided by the Treasury Board Secretariat to identify key issues in the security policy that should be included in an institution's audit program.

After the initial review in 1987-88, institutions will conduct an internal audit of their compliance with the policy and the efficiency with which they are implementing it at least once every five years. In this connection, institutions may call upon the assistance of the Communications Security Establishment in respect of communications-electronic security, and the Royal Canadian Mounted Police in relation to physical and EDP security.

The Communications Security Establishment and the Royal Canadian Mounted Police may be required to report to the Treasury Board Secretariat from time to time on the state of communications-electronic security and of physical security across the government.

The Public Archives of Canada will incorporate comments on security measures in its annual report to Treasury Board Secretariat on the state of records management in the federal government.

On behalf of the Treasury Board Secretariat, the Public Service Commission will include personnel screening as part of their Staffing Audits.

.10.2 EDP inspections

Institutions, other than DND, must request an inspection of their data centers by the Security Evaluation and Inspection Team (SEIT) every five years. They must also consult SEIT when major changes are planned in their information processing systems.

Following the inspection, the SEIT will prepare a security evaluation report for the deputy head. Copies will also be made available, on request, to the Treasury Board Secretariat and the Security Advisory Committee.

Institutions, other than DND, shall advise the SEIT within six months of receipt of the SEIT report of their plan to deal with identified problems. Institutions shall thereafter provide SEIT with annual progress reports.

Inspection of private sector EDP facilities that involve the processing of classified or designated information on contract must be arranged through the Security Branch of the Department of Supply and Services. Following the inspection of the facility by the SEIT, an evaluation report will be provided to the Director, Security Branch, SSC, who will subsequently make the results available to the chief officer of the private sector organization. Institutions contracting for EDP services may obtain from SSC information on private sector EDP facilities that have been authorized to process classified or designated information.

.11 Enquiries

All enquiries regarding administrative aspects of this policy should be directed to Information Management Practices, Administrative Policy Branch, Treasury Board Secretariat.

All enquiries regarding the personnel aspects of this policy should be directed to Policies and Procedures Group, Personnel Policy Branch, Treasury Board Secretariat.

Enquiries on matters falling within the government-wide roles of institutions set out in this policy should be directed to the institution concerned.

Appendix A
Roles in implementing the security policy government-wide

Cabinet and senior Public Service committees

The Cabinet Committee on Security and Intelligence (CCSI), chaired by the Prime Minister, provides general policy direction on security matters. It receives advice from the Interdepartmental Committee on Security and Intelligence (ICSI), chaired by the Clerk of the Privy Council. The Security Advisory Committee (SAC), chaired by the Deputy Solicitor General, advises ICSI directly on all security matters other than those related to administrative and personnel policy.

The Treasury Board issues administrative and personnel security policies and standards pursuant to CCSI direction. It receives advice from the Treasury Board Senior Advisory Committee (TBSAC), chaired by the Secretary of the Treasury Board, on matters generally related to the management of the public service, and from SAC on security matters.

The Public Service Commission is responsible for:

- establishing the staffing policies and procedures necessary to fulfill the requirements of this policy and to expedite appointments to Public Service positions, consistent with the statutory obligations and limitations of the Public Service Commission;

- establishing and maintaining a Central Index of employees released, rejected, dismissed or discharged for cause from the Public Service;

- ensuring, to the extent specified in this policy, that their referral inventory contains records of reliability checks and reports of serious misconduct or performance adversely affecting reliability; and

- establishing security training programs, as required.

The Canada Employment and Immigration Commission is responsible for ensuring, to the extent specified in this policy, that their referral inventory system contains records of reliability checks and reports of serious misconduct or performance adversely affecting reliability.

The Canadian Security Intelligence Service is responsible for:

- investigating individuals, when requested, for the purpose of a security clearance;

- conducting subject interviews as part of the security clearance process, other than for DND;

- providing security assessments, as requested by deputy heads;

- maintaining a central index of security clearances; and

- establishing guidelines for the declassification or downgrading of classified information pertaining to intelligence activities, as defined in sections 12 to 16 and subsection 19(a) of the Canadian Security Intelligence Service Act, as well as that relating to intelligence sources or methods.

The Communications Security Establishment is responsible for:

(a) formulating communications-electronic security standards for the Government of Canada and advising on their application;

(b) providing advice and guidance on the planning, acquisition, installation and procedures for using communications-electronic security systems;

(c) inspecting, testing and evaluating communications-electronic security systems and procedures, other than for DND;

(d) on request, reviewing government telecommunications to assess adherence to prescribed communications-electronic security practices;

(e) providing cryptographic material and documentation to appropriate government institutions;

(f) classifying signals intelligence information and material and protecting such information and material under its control;

(g) advising on and inspecting the measures used by other institutions to protect signals intelligence information and material;

(h) establishing special procedures and practices for the systematic review of classified cryptographic information for declassification or downgrading;

(i) reporting to Treasury Board, when requested, on the state of communications-electronic security across the government;

(j) providing a research and development and evaluation capability on security aspects of computer hardware, software and communications systems to ensure that information is available to the government on the security of computer systems and their use in government.

The Department of Communications is responsible for:

(a) ensuring that the need for communications-electronic security is recognized by its clients;

(b) identifying communications and security requirements to customers, where such requirements are one element of a larger communications problem;

(c) acting as liaison between the Communications-Electronic Security Committee and government institutions that are not members of the Committee, and providing advice and guidance to those institutions, in consultation with the Communications Security Establishment; and

(d) ensuring the integrity and availability of the telecommunications it provides to the government.

The Department of External Affairs is responsible for:

(a) all measures to protect classified and other sensitive information and assets under its control in Canada, and at and between Canadian diplomatic and consular missions abroad;

(b) conducting or arranging the inspection of these measures;

(c) performing or arranging the inspection of measures used by other government institutions to protect classified information and other assets handled by its Canadian Diplomatic Communications Service (which includes diplomatic couriers) to ensure continuity and uniformity of protection;

(d) ensuring that adequate safeguards are accorded by all government institutions to North Atlantic Treaty Organization (NATO) documents under their control, and inspecting the custodial arrangements for such documents. The Department of National Defence, however, does its own inspections; and

(e) updating the security clearances of its personnel who are members of the rotational Foreign Service and who have served, or are serving, outside Canada. The CSIS will continue to provide assessments, when required.

The Department of National Defence. The Deputy Minister and the Chief of the Defence Staff are jointly or separately responsible, as appropriate, for:

(a) all aspects of security for defence works, establishments, facilities, assets, resources and operations, in Canada and abroad;

(b) safeguarding classified information and other assets under their control, including those provided by allied nations and organizations;

(c) arranging for and coordinating security for any Force visiting Canada, or otherwise present at a defence establishment or facility;

(d) verifying that government institutions holding documents containing atomic information exchanged in accordance with bilateral and multilateral agreements are safeguarding those documents as required by the agreements;

(e) conducting the security clearance of members and prospective members of the Canadian Forces and other individuals employed or about to be employed by, in or on behalf of DND, excluding the Communications

Security Establishment and Defence Construction (1951) Limited. Where a search of security intelligence records is required, the CSIS shall carry out this activity;

(f) inspecting and evaluating measures to safeguard its own EDP assets;

(g) developing security measures that meet the intent of the government-wide standards for military and related field operations or national emergencies; and

(h) the conduct of counter-intrusion and counter-intelligence programs within the department, in accordance with approved security standards and agreements.

The Department of Supply and Services is responsible for:

(a) advising on the acquisition of guard services and physical security equipment;

(b) acquiring such goods and services, and ensuring that the suppliers comply with approved standards, as outlined in a contract or agreement, throughout the life of that contract or agreement;

(c) ensuring that adequate safeguards are applied at off-government premises by non-government personnel or private sector organizations with access to or custody of classified assets during a pre-contractual process, or under a contract or agreement to provide goods or services through SSC to the government;

(d) providing advice and assistance to government institutions in implementing bilateral and multilateral industrial security agreements or arrangements;

(e) providing advice and guidance to government institutions on all aspects of the payments process under the control of the Receiver General and the Deputy Minister of Supply and Services. Such responsibilities include payments, documents design, procuring and safekeeping; protection of payment data; payment systems and procedures; accounting practices; and other related security matters;

(f) establishing the necessary policies and procedures to conform to this policy, including the screening, where required, of contractors providing goods or services through SSC to government departments and agencies; and

(g) informing potential contractors of the policy and related procedures.

The National Archives of Canada is responsible for helping institutions to apply the security policy to information holdings within the context of the government records management policy, and for addressing this issue in the National Archivist's annual report to Treasury Board on the state of records management in the Government of Canada. As well, the Archives is responsible for the systematic declassification and downgrading of information transferred to its control for historical or archival purposes.

The Royal Canadian Mounted Police is responsible for:

(a) developing government-wide physical and EDP security standards;

(b) inspecting, testing, evaluating and, where required, designing physical security equipment, and developing related specifications;

(c) maintaining, where required, physical security equipment uniquely designed or modified for the protection of classified information;

(d) when requested, reviewing and advising on physical security arrangements in government institutions;

(e) providing, on request, a security consulting service for the design of new or renovated government buildings or the application of physical security equipment or systems to help institutions to satisfy their protection responsibilities;

(f) when requested, reviewing and advising on EDP security in government institutions, other than for DND, and in the private sector where it is engaged in processing government information under contract through the EDP Security Evaluation and Inspection Team (SEIT). SEIT is organized and administered by the RCMP but draws on interdepartmental resources, where practicable;

(g) when requested, reviewing measures in place in government institutions to prevent technical intrusion, and initiating related government-wide standards;

(h) reporting to the Secretary of the Treasury Board, when requested, on the state of physical security across the government, and annually, on the security status of all EDP facilities in government institutions (SEIT Report);

(i) helping to determine the suitability of persons for reliability or security clearance, by checking criminal records and providing details of any adverse information to the CSIS, in the case of security clearances, to DND in respect of its own security clearances, and to departments in the case of reliability checks;

(j) conducting the security clearance of members and prospective members of the RCMP, other individuals employed or to be employed by or in the RCMP, and persons employed under contracts awarded or administered by the RCMP. Where a search of security intelligence records is required, the CSIS shall carry out this activity; and

(k) carrying out specialized training on physical and EDP security, either directly or with the assistance of other government institutions, as required and mutually agreed upon.

Appendix B

Guide to seeking advice on protective measures and other aspects of security policy

AREAS	ORGANIZATIONS						
	CSIS	CSE	SSC	RCMP	TBS	ARC	PCO
. Physical security				X			
. EDP security				X			
. Communications-electronic security		X					
. Personnel security	X				X		X
. Access and privacy practices					X		
. Records management practices						X	
. Acquisition process			X				
. Industrial security			X				
. Payments process security			X				

Points of contact:

- Deputy Commissioner, Operations (Protective), Royal Canadian Mounted Police
- Director General, Communications Security, Communications Security Establishment
- Information Policy, Administrative Policy Branch, Treasury Board Secretariat
- Intelligence and Security Secretariat, Privy Council Office
- Personnel Security, Personnel Policy Branch, Treasury Board Secretariat

Points of contact: (Cont'd)

- Director General,
  Records Management Branch,
  National Archives of Canada

- Security Adviser,
  Department of Supply and Services

- Security Screening
  Services,
  Canadian Security
  Intelligence Service

Appendix C
Principles for declassifying and downgrading information

Information shall be declassified or downgraded in classification only by employees acting in accordance with authority conferred in their institution's information classification guide, or by those officials named by the deputy head as having authority to classify information not governed by such a guide. No institution shall declassify or downgrade the classification of any information originating in another institution or government without prior consultation.

At the time the information is created or collected, institutions shall provide, when possible, for automatic declassification and downgrading by setting a specific date or event at which declassification or downgrading is to occur.

Institutions shall declassify and downgrade the classification of other information by means of systematic review, in accordance with guidelines they develop for this purpose. Information deemed by the Archivist of Canada to have permanent value to the nation, and which is classified when transferred to the Archives, shall be safeguarded at the applicable level at the Archives while such protection is required. It shall then be declassified under an agreement with the institution transferring the information.

When requests are received under the Access to Information Act or the Privacy Act for records that have been classified, institutions shall carefully review such records in order to determine whether or not exemptions should be invoked. A decision to deny access to a record, or any part of it, must be based solely on the exemption provisions of the Acts as they apply at the time the request is made, and not on a security classification or other designation, however recently it may have been assigned.

Where review of compliance with this policy determines that information has been classified when it should not have been, classified at a higher level than necessary, or classified properly but its sensitivity has since disappeared or diminished, the information shall be declassified or downgraded in accordance with direction from the deputy head.

Declassification or downgrading shall be annotated on the information concerned to show the date of the action (if not already recorded at the time the information was classified), and the level to which the classification is downgraded in cases where information originally classified as TOP SECRET or SECRET no longer requires safeguards at the higher level.

Appendix D
Exemption provisions and designations relating to sensitive information outside the national interest

	Exemption provisions	Designations Mandatory - Optional
(a)	Law enforcement and investigations, where these do not relate to the national interest (s.16, ATIA; s.22 and s.24, Privacy Act)	PROTECTED - Law Enforcement
(b)	Safety of individuals (s.17, ATIA; s.25, Privacy Act)	PROTECTED - Individual Safety
(c)(i)	Competitive position of government (para.18(b), ATIA)	PROTECTED - Government Competitive Position
(ii)	Government Research (para.18(c), ATIA)	PROTECTED - Government Research
(iii)	Undue benefit to a person (para.18(d), ATIA)	PROTECTED - Undue Benefit to a Person
(d)	Third party (business) information (s.20, ATIA)	PROTECTED - Business Information
(e)	Testing procedures, tests and audits (s.22, ATIA)	PROTECTED - Tests/Audits
(f)	Solicitor-client privilege (s.23, ATIA; s.27, Privacy Act)	PROTECTED - Solicitor-Client Privilege
(g)	Information obtained in confidence from other governments (s.13, ATIA; s.19, Privacy Act)	PROTECTED - Other Governments
(h)	Medical records (s.28, Privacy Act)	PROTECTED - Medical

	Exemption provisions	Designations Mandatory - Optional
(i)	Advice etc. relating to non-national interest-sensitive matters (s.21, ATIA)	PROTECTED - Advice
(j)	Certain statutory provisions prohibiting the disclosure of information which does not relate to the national interest (s.24 and Schedule II, ATIA)	PROTECTED - (the statute) e.g. - Statistics Act - Income Tax Act
(k)	Personal information, as defined in section 3 of the Privacy Act, respecting members of the general public	PROTECTED - Personal Information
(l)	Particularly sensitive personal information	PROTECTED - Sensitive Personal Information
(m)	Personal information respecting federal employees of a nature described in (k) above	PROTECTED - Employee Information
(n)	Cabinet confidences, as defined in ss.69(1) of the ATIA and ss.70(1) of the PA, which are not part of the Cabinet Papers System and do not otherwise qualify for classification in the national interest	PROTECTED

Appendix E
Elements of the Personnel Screening and Security Clearance System

ELEMENTS	RELIABILITY		SECURITY		
	BASIC	ENHANCED	LEVEL 1	LEVEL 2	LEVEL 3
Verify Personal Data	X	X	X	X	X
Verify Education/Professional Qualifications	X	X			
Verify Employment Data	X	X			
Employment Reliability References	X	X			
Personal Character Reference			X	X	X
Criminal Records Name Check*	X				
PSC Central Index Check	X	X	X	X	X
Fingerprint Check	MAY BE REQUIRED	X+	X	X	X
CSIS Indices Check			X	X	X
Field Investigation of 10 years background or to age 18 (whichever comes first)			FOR CAUSE[1]	FOR CAUSE[1]	X[2]
Credit Check		Xx	X	X	X
Subject Interview			To be implemented on a pilot basis for security clearances		

* If a name check indicates a criminal record, the record cannot be released without first receiving the fingerprints as positive identity.

\+ For current federal government employees, may be replaced by a criminal records name check at the discretion of the deputy head.

x When the duties or tasks to be performed, in the opinion of the deputy head, require it.

1. "FOR CAUSE" means "The investigating agency will determine, based on available information, whether a greater degree of screening is required".

2. Field investigation of 20 years' background or back to age 18, (whichever comes first), is required for access to special material, in accordance with international agreements.

Appendix F
Key Requirements for Personnel Screening

Reliability Checks

(a) Information to assess qualifications often comes from the same source as that to assess reliability. In these situations, the information for both should be gathered concurrently.

(b) All candidates for appointment or assignment, who will be subject to a reliability check, must be informed:

- that their employment, personal history and educational qualifications will be verified;
- of the possible consequences of this verification and of making false statements; and
- of their rights in this process as outlined in this policy (see (g) and (h) of this section, and section .8.2.1 of the policy).

(c) In order to be considered for an assignment involving a reliability check or security clearance, individuals will be requested to sign TBS Form 330-58 (86/08) "Consent to Disclosure of Personal Information". Such disclosures are governed by the provisions of the Privacy Act.

(d) In a staffing process, checks should normally be conducted only on those about to be offered an appointment.

(e) Personal and educational data will normally require verification once only. Other elements of a reliability check may require updating.

(f) To avoid unnecessary workload, maximum use should be made of information about the candidate that is already available.

(g) A individual must be given an opportunity to explain adverse information before a decision is reached.

(h) Employees must be given the reasons why they have been denied an appointment or assignment, unless the information is exemptable under the Privacy Act.

(i) When an incumbent employee does not meet the requirements of the enhanced reliability check required by his or her position, the employee shall be informed of his or her rights of redress as specified in section .8.2.1 of this policy.

(j) The manager must complete and sign TBS Form 330-71 (86/09), verifying that the checks have been carried out and that, in his or her best judgement, the risks attached to making the appointment or assignment, based on the level of reliability required by the duties to be performed, are acceptable or not. Managers shall be accountable for such decisions.

(k) Records of such decisions and the information upon which they are based must be retained, normally as part of the staffing file.

(l) Information gathered by departments conducting reliability checks on given persons referred from a Central Inventory (PSC or CEIC) shall be passed to the referring agency, except where the person has been appointed to an indeterminate position.

(m) For persons referred from a Central Inventory and subsequently employed on a term basis, any serious misconduct or performance adversely affecting reliability must be reported to the referring agency in a manner prescribed by the agency (PSC or CEIC), even if the duration of appointment is less than six months and the optional basic reliability check has not been carried out.

(n) Managers shall inform contracting authorities, either departmental or central, of the reliability requirements of the tasks to be performed.

(o) Where a contract is involved, it shall stipulate that individuals performing the work must have met the requirements of a basic reliability check or enhanced reliability check as appropriate before they commence work.

(p) The criminal records name check and the credit check are to be conducted by the approved agencies through the Departmental Security Officer (DSO).

(q) A basic reliability check, where the policy requires such a check, must still be conducted even when a security clearance is needed. The resulting information is to be forwarded through the DSO to the investigative body. In such instances, however, the criminal records check will be the responsibility of the investigative body.

Appendix G
Conditions relating to Security Clearances

(a) Where a reliability check has been conducted before a security clearance request, information gathered as result of this check shall be forwarded through the Departmental Security Officer (DSO) to the investigative body. Security clearance investigations will be carried out by the Canadian Security Intelligence Service, with the exceptions noted in the roles of the Royal Canadian Mounted Police, Department of National Defence and the Department of External Affairs (see Appendix A). Requests for security clearances will be made through Departmental Security Officers on TBS form 330-23 (86/09), "Security Clearance Request and Authorization".

(b) In order to be considered for an assignment involving a reliability check or security clearance, individuals will be asked to sign TBS Form 330-58 (86/08) "Consent to Disclosure of Personal Information". Such disclosures are governed by the provisions of the Privacy Act.

(c) Managers shall inform contracting authorities (departmental or central) of the security requirements of the tasks to be performed.

(d) When contracting for goods or services involving access to classified information and assets the contract shall stipulate that individuals needing such access to perform the work shall have a security clearance at the appropriate level before they commence work.

(e) Persons should be denied a security clearance if there are reasonable grounds to believe that:

- they are engaged in, or may engage in activities that constitute a "threat to the security of Canada", as that term is defined in the Canadian Security Intelligence Service Act (definition is attached to this Appendix);

- because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties of affection to persons living in oppressive or hostile countries:

  . they may act or may be induced to act in a way that constitutes a "threat to the security of Canada", as defined; or

  . they may disclose, may be induced to disclose or may cause to be disclosed in an unauthorized way, government information classified in the national interest.

(f) A decision to grant or deny a security clearance must be based on adequate information. Where such information does not exist or cannot be obtained, a security clearance cannot be given. An assessment that indicates that no information is available about

an individual, or that covers only a very short period of his or her life, does not provide adequate grounds on which to base a security clearance.

(g) When a deputy head has denied or revoked a security clearance, the individual must be informed according to sub-section 42(1) and (2) of the CSIS Act.

(h) Individuals who have been granted a security clearance shall be briefed on their security responsibilities and shall sign TBS Form 330-47 (86/4) "Security Briefing and Declaration".

A "Threat to the Security of Canada" includes:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada, or activities directed toward or in support of such espionage or sabotage;

(b) foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state; and

(d) activities directed toward undermining by covert unlawful acts, or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada.

It does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d) immediately above.

Appendix H
Cabinet Papers System

The records administered under the Cabinet Papers System (excluding records pertaining to the Treasury Board), and drafts of these records, include:

Memoranda to Cabinet
Records of Cabinet Decision
Aides-mémoire
Committee Reports
Draft Legislation (e.g. bills and regulations)
Cabinet minutes
Committee minutes
Draft Orders-in-Council and Schedules thereto
Ministerial Submissions to the Governor in Council and Explanatory Notes
Draft Ministerial Orders
Briefing Notes for Committee Chairmen and Members
Agendas of Cabinet and Cabinet Committees

Appendix I
Treasury Board Papers System

The records administered under the Treasury Board Papers System, and drafts of these records, include:

Submissions to the Treasury Board
Extracts from the Minutes of Meetings of the Treasury Board
Treasury Board Minutes
Treasury Board decision letters
Treasury Board agendas
Draft Orders-in-Council
Briefing notes for the Treasury Board (précis)

Appendix J
Key references

Legislation

Access to Information Act
Canadian Security Intelligence Service Act
Financial Administration Act
Official Secrets Act
Privacy Act
Public Service Employment Act
Public Service Staff Relations Act

Government Policy

Administrative

Interim Policy Guide: Access to Information Act and the Privacy Act (Treasury Board)

Materiel Custody (Treasury Board, Administrative Policy Manual, Chapter 226)

Materiel Security (Treasury Board, Administrative Policy Manual, Chapter 218)

Personnel

- Staffing volume (Treasury Board, Personnel Management Manual, Vol. 6)
- Policy on discipline (Treasury Board, Personnel Management Manual, Vol. 7, Chapter 7)
- Terms and conditions of employment overview (Treasury Board, Personnel Management Manual, Vol. 8)