SECRET

DRAFT

MEMORANDUM TO CABINET

MÉMOIRE AU CABINET

Security of Personnel - Government of Canada

and

Protection of Government of Canada Assets

Solicitor General of Canada

Solliciteur Général du Canada

## EXECUTIVE SUMMARY

### ISSUE

Whether to resolve existing problems and to complement recent related government activities by approving new policies to replace personnel security policy dating from 1963, and classification policy for the protection of sensitive government assets, dating from 1956.

### RECOMMENDATIONS

It is recommended that:

1. TB be authorized to issue and amend Operational Policies, directives and guidelines for Security of Personnel and Protection of Government of Canada National Interest Assets in accordance with the recommendations and proposals in this Memorandum.

2. The Treasury Board and Public Service Commission examine and prescribe a system of verification for trustworthiness and essential suitability of all public service employees as required by the nature of their duties (MC, p. 15, paras. 10, 11).

3. This personnel security policy apply to all government and non-government personnel whose duties may afford an opportunity to cause injury to the safety and integrity of Canada (MC, pp. 15,17, paras. 13-15), except for such cases as O-i-C appointees (MC, p. 17, para. 16).

4. Criteria for three security clearance levels and appropriate screening procedures be established (MC, pp. 17-21, paras. 17 to 25 and Annex I).

5. Persons should be denied a security clearance if there are reasonable grounds to believe that:

(a) they are engaged in or may engage in activities which constitute a "threat to the security of Canada" as that term is defined in the CSIS Act;

(b) because of features of character, or association with persons or groups referred to in (a) above, or through 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 such a way as to constitute a "threat to the security of Canada", as defined.

6. A security classification system be authorized for the protection of National Interest information with appropriate designators and injury tests (MC, pp. 25, 27, paras. 34-42 and Annex VI).

7. TB be authorized to develop procedures for the safeguarding of other categories of sensitive, non-security, information for later consideration (MC, p. 27, para. 40).

8. The ultimate responsibility of deputy heads for security in their government institutions be confirmed (MC, pp. 19 and 27, paras. 22 and 44).

9. The miscellaneous recommendations be approved (MC, pp. 27, 29, paras. 43, 44, 46-49).

RATIONALE

10. Dated security clearance policies have been criticized. They should reflect current security requirements and provisions of the CSIS Act. New criteria for a security clearance to determine loyalty to Canada and associated reliability are needed.

11. Evidentiary criteria for denial of a security clearance should be brought in line with "threats to the security of Canada", as defined in the CSIS Act.

12. The existing classification system for information, developed during WW II, has lost its integrity and effectiveness. New criteria and injury tests for classification are required to protect National Interest information. Indeed, some departments have moved to establish their own protection programs, in the absence of new policy.

13. Since one of the criteria for a security clearance is access to security classified information, the new classification system will play a part in determining the need for security screening.

POSSIBLE ADVERSE CONSEQUENCES

14. Misplaced criticism of the government strengthening the already extensive surveillance powers of CSIS, invading citizens privacy, restricting freedoms, infringing on Charter Rights and of the capacity to bar some persons from government employment.

15. Uninformed criticism that changes would undermine the access and privacy laws.

DEPARTMENTAL POSITIONS

16. The recommendations have been reviewed by ICSI and consultation was held in the Security Advisory Committee. There is agreement on the recommendations except that some departments favour evidentiary standards for rejection based instead on the probability of the security threat (MC, pp. 21, 23, paras. 30 and 31).

POLITICAL CONSULTATIONS

17. Caucus: Information not available.

18. Party/Other: Information not available.

COMMUNICATIONS

19. Plan: Synopsis follows.

20. Major Theme: Security clearance criteria and screening procedures urgently require revision to orient them toward "threats to the security of Canada and to eliminate misuse of screening. Present classification policy is outdated and misused.

COMMUNICATIONS
SYNOPSIS

| DOCUMENT TITLE | SECRET (when completed) |
|---|---|
| SECURITY OF PERSONNEL - GOVERNMENT OF CANADA and PROTECTION OF GOVERNMENT OF CANADA ASSETS | DATE |

STRATEGY

1. Objective(s)To inform the public of new policy for: (1) security screening and clearances for public servants, persons seeking public service jobs and persons in other sectors under contract to the government, where the nature of the work requires a security clearance; (2) protection of sensitive government information and assets relating to Canada's national security.

2. Major Themes 1) Revisions to security clearance policies are urgent. Existing policies are outdated and have been criticized. New policies for clearances and denial of clearances are designed to withstand critical scrutiny. Canadians must know that persons occupying sensitive positions are loyal. The CSIS Act provides redress through the Security Intelligence Review Committee for persons denied a clearance. 2) Former classification procedures have been misused - national security information must be protected properly.

3. Impact and Anticipated Reaction
a) Special Interest groups
1) Some might claim screening is intrusive, will further restrict Charter Rights and increase CSIS power. Unions will likely adopt a "wait and see" stance. 2) Some may claim an attempt to restrict access rights and new government secrecy. Public Servants will welcome the clarification.
b) General Public/other
The general public and media would probably agree the personnel policies are needed and overdue, and acknowledge the existence and importance of the statutory review powers of SIRC. Most will agree that sensitive information must be safeguarded, but some will ask if access rights are being abrogated.

ANNOUNCEMENT

4. Method
A press release, an outline of the new policy thrusts, highlights and background notes.

5. Place(s)
Ottawa

6. Specific Target Group(s)
1) Public Servants, potential federal employees and federal government contractors.
2) Rights groups.
3) Investigative journalists.

7. Participants

RESOURCES

8. Support Materials
None

9. Total Communications Budget
Within current budget.

ADDITIONAL INFORMATION

10. The Operational Policies would be issued at a later date by Treasury Board, accompanied by necessary directives and guidelines.

PCO/BCP 135 (Rev 07/81)

DRAFT MEMORANDUM TO CABINET

BACKGROUND

1. Administrative security within the Government has traditionally been based on two key policies, personnel security screening and the classification/physical protection system for sensitive assets. Currently security screening is governed by Cabinet Directive 35 (CD35), 1963, which was declassified in 1978. The 1956 PCO document, "Security of Information in the Public Service of Canada" ("Security of Information - 1956"), is the primary document governing classification of information. There has been unjustifiable misuse and, indeed, abuse of the personnel security screening system which has led to human rights criticisms and to a wasteful use of government resources. The security classification system has also been misused to classify other than national security information, impairing the effectiveness of measures to protect sensitive government information and leading to unwarranted security screening of individuals. Existing policies are not entirely consistent with the provisions of the CSIS Act.

2. Security of Personnel: CD35 sets out the principles and procedures for the determination of the loyalty and reliability of all persons who are to have access to classified information. More importantly, it illustrates those activities, beliefs and features of character which could be a bar to employment in the Public Service or which could be disqualifying factors for access to classified information.

3. In CD35, classified information is not defined. It is assumed, however, that CD35 was intended to protect from unauthorized disclosure the same vital defence and security information that was generally identified for classification in "Security of Information - 1956", since protection against injury to the state is the common principle. Over time, however, the classification system has been increasingly misused to protect information for which it was not intended. As a consequence, many public servants have been subjected to the security screening program to determine their loyalty when the information to which they had access should not have been classified.

4. Security of Information: "Security of Information - 1956" stipulates, in effect, that most official documents produced by the Government of Canada require some form of classification. It was developed during and after World War II to deal with information requiring protection from disclosure for vital defence and security reasons. The absence of an up-to-date and comprehensive security policy in the Government of Canada, especially one that deals with the classification of other categories of information, has led to misuse of the current classification system and has impaired the effectiveness of the measures used to protect sensitive Government information. It is clear that a significant amount of Government information is security classified when it ought not to be. The classification system for the protection of information has expanded beyond any supportable Government interest and has lost its integrity as a system.

5. Related Factors: The 1981 McDonald Commission Report criticized the slow pace of policy reform in government administrative security in response to identified priority problems. There has

also been repeated criticism from the Canadian Human Rights Commission (CHRC) concerning the over-use of personnel security clearances and unwarranted discrimination against certain groups inherent in the evidentiary criteria for rejection. Recent events such as the enactment of the privacy and access legislation and the creation of the Canadian Security Intelligence Service (CSIS) have reinforced the need for policy reform.

6. The CSIS Act created the Security Intelligence Review Committee (SIRC), which affords a statutory review in cases where a security clearance is denied. Ministers should be aware that immediate action will allow the government to make its own conscious policy decisions on new administrative security policies for clearances and classification, rather than being placed in a reactive position at a later date based on unfavourable conclusions flowing from a SIRC review.

7. Major Problems: A major review has revealed that new administrative security policies must be implemented to address the following fundamental issues of concern:

(a) For personnel security:

(i) security screening is often misused as a substitute for basic personnel reference checks for prospective employees;
(ii) CD35 lacks clarification of those circumstances, beyond access to classified information (itself not defined), for which a security clearance is required;
(iii) CD35 does not adequately address what level of clearance is required to ensure the protection of the state's interest;
(iv) CD35 fails to specify appropriate investigative procedures required, consistent with the security clearance levels;
(v) CD35 loyalty criteria are stated in narrow, non-contemporary terms and its reliability criteria lack, in the main, any causal connection to the risk factors threatening national security;
(vi) the current evidentiary criteria for denial of a security clearance are not uniformly and consistently applicable;
(vii) existing policy on separatist activity, as it relates to security clearance, is ambiguous.

(b) For protection of sensitive assets:

(i) "Security of Information - 1956" prospectively requires that most Government information be security classified and it fails to distinguish personal or private information from that related to the security of the state;
(ii) the use of the current classification system to protect other than national security information had led to a wasteful use of resources and inappropriate security screening of individuals.

(c) For management of administrative security:

(i) no single accountable responsibility centre exists.

OPTIONS

8. There are three main options:

(a) maintain the status quo;
(b) authorize new policy principles governing the security of personnel and information, as further described in this Memorandum;
(c) consider whether the proposal in paragraph 29 should be modified in accordance with the alternative in paragraphs 30 and 31.

I. SECURITY OF PERSONNEL

9. General: Good personnel management requires the examination of the trustworthiness and suitability of all employees to protect the employer's interests, usually involving reference enquiries, verification of qualifications and often credit and criminal history checks. A national government, in addition, must have regard for the employee's loyalty and associated reliability as those relate to national security concerns.

10. Verification of Suitability - Employment Practices: Formal and mandatory checks of qualifications, previous employment and references are indispensable in the staffing process and should be strengthened to eliminate the current misuse of security screening. They are also prerequisites to effective security screening. It is proposed that policies be developed by TB and PSC to ensure that, for all positions, there is documentary verification of identity, citizenship status, qualifications and address; and telephone or written verification of general suitability through inquiries with previous employers, education and references and, where appropriate, criminal indices and credit checks.

11. For persons whose duties would never require or permit access to security classified information or would not justify their being security screened for other reasons, there would be no security screening. Implications resulting from this approach are further dealt with in para. 21. The proposed verification of trustworthiness and suitability would constitute an important personnel management check, would result in savings in financial and human resources and would avoid political difficulties because there would be fewer cases of security screening and less instances of its being used without justification. It would not constitute a security clearance. It is expected, however, that where CSIS has any information of a significant nature bearing on a hiring decision, the appropriate hiring authority could be informed. The decision to provide such information would be made by the Solicitor General in accordance with Section 19(2)(d) of the CSIS Act. The use of Section 19(2)(d) is discussed in paragraph 33.

12. Non-classified information can continue to be protected through appropriate administrative arrangements. In addition, public servants will continue to be required to obtain authorization to release any government information, including that which is not classified. This responsibility can be enforced through disciplinary and, where appropriate, criminal sanctions. Ministers should also expect a separate MC from the Treasury Board dealing with administrative sanctions.

13. The Scope and Application of Security Screening: Security screening currently exists to allow access to classified information. It is the traditional purpose of personnel security screening to prevent the unauthorized disclosure of security classified information and this supports the application of the most disciplined and complete screening procedures to those persons with access to such information. A second consideration, highlighting the need for security screening, beyond those who have direct access to classified material, concerns those persons, for reasons relating

to the particular nature of their work, whose positions may afford an opportunity for an incumbent to cause injury to the integrity and security of the state through proximity to people, places, or property relating to national interest. It is therefore recommended that the proposed new personnel security screening policy should apply to those persons occupying positions, whose duties may afford an opportunity for an incumbent to cause injury to the national interest through access or proximity to people, places, property or information relating to such interests. Examples of such positions are given in Annex I.

14. The concern for safeguarding national security requires that the resources of the CSIS be used to conduct a disciplined screening process, as recognized by the Service's legal mandate to prepare security assessments for government institutions. The requirement for such screening must be interpreted in a judicious way to ensure that the system is not abused. DND and the RCMP will perform their own security clearance procedures in accordance with the other provisions of this policy.

15. The policy should apply to all persons in the Federal Government and the private sector who, through the nature of their work or by agreement or contract, fall within the above criteria. A security clearance is to be considered a condition of employment for specified positions and the consent of the individual must be obtained in advance of security screening.

16. Special Cases: Special circumstances may justify screening an individual who may not have access to national interest information, but will be in a position to observe, influence or particpate in events of national significance. An example would be O-i-C appointees. This policy area is best left to Prime Ministerial instruction with the necessary involvement of PCO and other agencies.

17. Security Screening Levels: Paragraph 13 of this MC proposes an extended scope for security screening. Not all positions in the government afford an equal opportunity to affect the state's interests. Some are much more sensitive than others. It is important to determine what level of clearance is required to ensure the protection of the state's interests in balance with the minimum, justifiable intrusion into an individual's rights. For these reasons, it is proposed to highlight the change by introducing a new set of titles for security clearances and screening procedures - LEVEL I, LEVEL II and LEVEL III.

18. To permit proper and consistent assignment of security clearance levels to positions, and thereby trigger the various CSIS screening procedures on a cost-effective basis relative to the threat, the following definition is proposed:

- A LEVEL I, II or III security clearance requirement shall be fixed for positions which may afford an opportunity for an incumbent to cause specific and identifiable, respectively, injury, serious injury or exceptionally grave injury to the National Interest* through access or proximity to people, places, property or information relating to such interests.

  * NOTE: National Interest relates to the defence and maintenance of the social, political and economic stability of Canada and thereby, the security of the nation.

19. The wide variety of occupations in government institutions and the differing physical environments and working relationships in which duties are performed, make it impossible prior to the implementation of the new policy, without a total position-by-position examination, to set out any definitive allocation of positions to the three proposed security clearance levels. Nor is it possible to predict with any degree of precision how many positions will require any level of security clearance, but the system is predicated on the basis that the screening is totally justifiable.

20. Further assistance to government institutions in applying the three levels of security clearance, would be issued by TB in guidelines. For purposes of illustration and to facilitate consideration by Ministers of the impact of the policy framework, Annex I sets out sample positions falling within one of the three clearance levels and also describes relevant screening procedures.

21. The proposed criteria would not require that the majority of public servants be security screened. In that sense it can be argued that someone who may be considered disloyal to Canada could be employed in a position not requiring a security clearance. Even though the CSIS Subversive Indices might contain information on that person, the information therein would not be retrieved or assessed since no security screening would be required. This same possibility exists under CD35 and the consequences currently might well be more serious than under the proposed system owing to the deficiencies in present criteria for identifying positions requiring a clearance. The proposed criteria clearly identify and justify security screening in cases where it might reasonably be expected that the duties of a position could afford an opportunity for a person to cause injury to Canada's interests. In any event, where CSIS comes into possession, during the normal exercise of its mandate, of adverse information which reflects on a person in the public service or seeking employment therein, it is the view of legal counsel that such information could, in some circumstances, be disclosed to the relevant authority in accordance with the exceptional provisions of Section 19(2)(d) of the CSIS Act. The provisions of Section 19(2)(d) are discussed in paragraph 33.

22. Deputy heads will be required to exercise the responsibility to fix and review security clearance levels continuously in accordance with the criteria and changing circumstances. This will allow the modification of the security clearance level of a position at any time if circumstances warrant. They will also have the responsibility to decide who is to be granted a security clearance and who is to be denied a security clearance after receiving expert advice from CSIS in the form of a security assessment as required by the CSIS Act.

23. Security Screening Procedures and Subject Interviews: CD35 sets out three levels of security clearance. Procedures for granting Confidential or Secret clearances, however, are identical, involving only a check of criminal records and security indices. Security screening for these two levels reveals virtually nothing about the reliability of an individual beyond a criminal conviction. Top Secret clearances involve records checks supported by a full field investigation in which various sources are interviewed. Clearly, screening currently conducted for a Top Secret clearance carries the best chance of revealing information relevant to both the loyalty and reliability of individuals.

24. The U.K. employs an additional screening procedure, in addition to field investigations, for higher levels of clearance, involving a searching interview of the individual by trained inter-

viewers. A recent controlled test by the US Department of Defence compared results of full field investigations against those of intense interviews intended to reveal evidence of subversive association or character factors. The products of field investigations and interviews were compared and it was found that the interviews revealed three times as much significant information as did field investigations.

25. The McDonald Commission recognized the value of the interview and recommended that it be adopted as a screening measure by CSIS, and also by DND and RCMP for their own employees, for the equivalent of Secret and Top Secret clearances. It is proposed that this technique now be authorized and phased in as an additional screening procedure for Levels II and III checks, at the discretion of the responsible Deputy Minister, initially on a selective, pilot basis within departments in order to test and refine the procedure. Ministers will wish to consider fully any later extension of this technique. Additional resources that would be required to comply with the McDonald recommendation may be costly given that each new or updated clearance would involve an interview and subsequent assessment. Update procedures and frequency for the interview and field investigations would be subject to change from the current situation to free resources to conduct new procedures. Revised procedures for Levels I to III checks will be found in Annex 1.

26. Security Clearance Criteria - Loyalty and Reliability: The loyalty and reliability criteria in CD35 are flawed (Annex II). The loyalty rejection criteria are not confined to "threats to the security of Canada" as defined by Parliament in the CSIS Act, but are rooted in narrow, non-contemporary terms. The McDonald Commission argued that the current system based on CD35 placed, and continues to place, the security agency in the untenable position of being required to provide a security assessment which would not be in conformity with the "threats to the security of Canada", as defined.

27. The CD35 reliability criteria were also criticized by McDonald because they did not connect reliability factors directly to "threats to the security of Canada". Experience shows that features of character have often been viewed subjectively and in isolation from any possible effects on Canada's security. A person's features of character, such as homosexuality, may, in certain circumstances, make him unsuitable for a particular post but do not necessarily mark him as disloyal. The importance of features of character for security clearance purposes cannot be over-emphasized. Most cases in recent years involving unauthorized disclosure of government secrets in NATO countries have involved these factors rather than ideological motives.

28. It is proposed therefore, that there must always be an objective assessment of loyalty and associated reliability factors to identify a possible connection with a "threat to the security of Canada" and to determine if these factors exert such influence that the individual may act disloyally. This proposal is confirmed by the definition of "security assessment" in the CSIS Act.

29. Rejection Criteria - Evidentiary Tests: There is an important decision to be made in determining the evidentiary standard to be used by deputy heads in making the decision to deny a person a security clearance. The McDonald Commission recommended an evidentiary standard based upon "reasonable grounds to believe." Since no distinction was drawn between its recommendation and CD35, it is fairly concluded that the Commission saw no conflict between

its recommendation and the current practice. It is therefore proposed that persons should be denied a security clearance if there are reasonable grounds to believe that:

(a) they are engaged in or may engage in activities which constitute a "threat to the security of Canada" as that term is defined in the CSIS Act;
(b) because of features of character, or association with persons or groups who are referred to in (a) above, or through family or other close ties of affection to persons living in oppressive or hostile foreign countries, they may act or may be induced to act in such a way as to constitute a "threat to the security of Canada" as defined.

The CSIS Act definition of "threats to the security of Canada" may be found in Annex III.

30. It may be argued that the terms "may engage in" or "may act or may be induced to act" in 29(a) and (b) above represent a standard that is inappropriate, in that they relate to a possibility rather than a probability that a person will act in a way that will constitute a threat to the security of Canada. An alternative would be to replace the words in (a) "may engage in" with "are likely to engage in", and in (b) to replace "may act or may be induced to act" with "are likely to act."

31. In considering the merits of the alternative, it should be taken into account that McDonald did recommend the alternative in para. 30 and that the Citizenship Act, Section 17.1(2), amended with the passage of the CSIS Act, requires a test of "reasonable grounds to believe that a person will engage in activity that constitutes a threat to the security of Canada...." Also, the Immigration Act at s.19(1) provides that "no person shall be granted admission if he is a member of any of the following classes: (e) persons who have engaged in or where there are reasonable grounds to believe will engage in acts of espionage or subversion against democratic government...." Further the CHRC which hears complaints regarding bona fide conditions of employment, except for security matters which are reviewed by SIRC, has issued guidelines under the CHRA requiring that "... the employer shall show that the exposure of the person to the risk would likely result in the disruption of the employer's business."

32. Security Clearance Criteria - Separatism: CD35 does not mention separatism, but a Cabinet decision of May 27, 1976, made public by the McDonald Commission, says separatism is a factor to be reported on in security screening as relevant to national security. That Cabinet decision, set out in Annex IV, provided that any relevant information concerning separatist activities, from whatever source, which could be substantiated could be used in decisions relating to the employment of persons in sensitive positions in government, including those for which a security clearance was required.

33. An analysis of McDonald's arguments and an examination of the principles underlying screening policy suggests that separatism per se does not constitute a threat to the security of Canada and should not be a factor when determining loyalty or associated reliability. Therefore, the simple fact of separatist affiliation, of holding separatist views or subscribing to separatist ideologies is not in itself, a security threat and, thus, these factors are not sufficient by themselves to question a person's eligibility for a security clearance. It is therefore proposed that the Cabinet

Decision of May 27, 1976 be deemed inoperative. Where information involving separatist activities is directly relevant to a determination of loyalty or reliability in respect thereof, it will be included in a security assessment by CSIS in accordance with Section 19(2) of the Act. Beyond this, information concerning separatist activities or support that do not constitute a threat to the security of Canada may, however, be relevant in certain circumstances to the question of a person's basic suitability to be employed in certain positions. In such cases, it is proposed that, where the information is voluntarily provided or is obtained during a routine verification of qualifications, it may be used by departmental authorities for consideration in the overall context of the person's assessment for employment in positions in which particular aspects of reliability and trust are primary concerns. The passing of this information could be accomplished only with the approval of the Solicitor General under the exceptional provisions of paragraph 19(2)(d) of the CSIS Act. The test to be applied by the Solicitor General under the Act is whether passing that information "... is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure ...." It should be noted that any such action by the Solicitor General must be reported to SIRC.

## II. PROTECTION OF ASSETS

34. General: The current policy for safeguarding government information contains two fundamental weaknesses. Originators of information are not provided with clear and simple direction as to what information should be security classified in order to protect national security interests. The second weakness is that there is no provision made for the classification of other than national security information thereby inducing the use of a security classification system for other kinds of sensitive government information. The general effect is a constant distortion of the security classification system with equally important adverse implications for the security screening program.

35. The current system of security classification is graphically depicted in Annex V. It should be noted that the classification designator RESTRICTED is not a security classification because no injury test is involved. It appears therefore to be inconsistent with the protection of the other three classification tests for TOP SECRET, SECRET and CONFIDENTIAL.

36. A Classification System for the National Interest Assets: The proposed classification plan features a National Interest category generally limited to the designation of information that could adversely affect the defence and maintenance of the social, political and economic stability of Canada and thereby the security of the nation. The proposed system is described in Annex VI and the subject areas covered are set out in the Note in para. 18.

37. Information identified for security classification in the National Interest requires a security level designation to signal to all persons having access to it that certain pre-determined protective measures must be employed since injury would be occasioned by its unauthorized disclosure. It is proposed that the existing designators - TOP SECRET, SECRET and CONFIDENTIAL - be used to identify the classification levels in the National Interest category of classified information, the term Confidential providing the threshold at which injury would be occasioned through unauthorized disclosure. It is proposed therefore that the term "RESTRICTED" be dropped, since, as has been demonstrated, it involves no injury test.

38. A procedural instruction in the operational policy will permit DND and other departments to properly safeguard Restricted material originating in other nations. Departments of the Government of Canada will no longer originate material classified as Restricted.

39. Given the adoption of the three current designators for the National Interest category, the following tests would apply:

- Government information shall be designated TOP SECRET, SECRET or CONFIDENTIAL when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause, respectively, exceptionally grave injury, serious injury or injury to the National Interest of Canada.

40. Other sensitive government information, essentially involving privacy and corporate confidences, would be safeguarded in accordance with separate procedures to be developed for later consideration by the TB. Such procedures would ensure that the national security category is not misused, as at present, to classify non-security material and would thus restrict inappropriate security screening. Information dealing with law enforcement, for example, would normally fall outside the National Interest category, but in cases of law enforcement information relating to the investigation of security offences, the information would fall within the National Interest category and would be assigned a National Interest designator to ensure it receives proper protection.

41. The proposal recommends itself since it decisively responds to the two fundamental weaknesses in the current system. It will provide clear direction to originators concerning the type of information that is to be security classified. It will also allow for the subsequent development of a system of identification for protection of sensitive private information other than national security information.

42. The clarification that this alternative would bring to the classification process, by specifying for the first time the general groupings and subjects of National Interest information, will eliminate the misuse of the current classification system.

43. Material Assets: The security classification of National Interest material assets (not currently provided) should be accomplished by applying the appropriate designators in a parellel fashion.

44. Control of Classification and De-Classification: Deputy heads should delegate the authority to classify to those officials with a need, and be responsible for reviewing and declassifying material in accordance with policies and directives.

## III - MANAGEMENT OF SECURITY POLICY

45. Current security policies and directives emanate from several sources, are outdated and inconsistent. Administrative security is a matter for central agency management. It is proposed that TB assume government-wide responsibility, under the FAA, by issuing the operational policies, directives and guidelines, covering assets protection, personnel, physical, communications-electronic, EDP and technical intrusion security. Deputy heads would be responsible for their departments' security. Roles of key departments and agencies would be confirmed in the operational policies.

46. Fingerprint Records: Private sector employees working on

classified contracts are not required to provide fingerprints for positive identification in RCMP criminal history checks. As is the case for public servants, they should be.

47. Status of Existing Directives and Instructions: Existing miscellaneous PCO instructions should be declared non-operative.

48. Central Index of Security Clearances: There is no central record of clearances in the current system. For records and updating purposes, there should be established and maintained a central automated index and all affected positions should be identified. The agency responsible for maintaining the index will be identified after a further review. CSIS is of the view that the index should be maintained by the Service.

49. Indoctrination Certificates and Non-Disclosure Agreements: The Department of Justice should review the current situation and look into the possibility of developing effective, non-disclosure agreements for persons with access to security classified information.

CONSIDERATIONS

50. Federal-Provincial and International Relations: The proposals do not affect personnel screening standards under international arrangements. Screening responsibilities on behalf of provincial governments, performed by arrangement under the CSIS Act, will be subject to agreed standards and procedures.

51. Impact on the Private Sector: Government contractors must observe classification, personnel and other security programs if classified assets are involved. Private sector security officers, with whom discussions were held in the development of these proposals, were of the view that a cost decrease for security measures for affected contractors might result. The new review process by the SIRC in cases where a security clearance is denied applies statutorily to private sector contractors and their employees by virtue of the CSIS Act. No such review procedure existed formerly.

52. Impact on Productivity: There may be general quantitative and qualitative increases in productivity, not capable of measurement at this stage. The security clearance criteria should result in a more cost-effective use of security screening resources. The proposal for the subject interview may prove quite valuable qualitatively for the purposes of CSIS in preparing security assessments for departments. The establishment of a central automated index of security clearances will simplify periodic updating of security clearances. Clearer instructions on National Interest classification and designators should expedite initial classification decisions by originators and also the appropriate selection of secure storage facilities.

53. Financial: It is not possible to specify resource costs involved in adopting the proposals relating to security screening or the new classification system, principally because no reliable cost yardstick exists that would apply.

54. There may be overall savings from:

i) reduced numbers of overall numbers of clearances and fewer costly field investigations;
ii) administrative savings result from the central clearance index;
iii) fewer requirements for costly physical storage and handling of security classified information;

iv) other economies in general security administration.

There may be some additional short-term and continuing costs, subject to later ad-referendum consideration by TB, resulting from:

v) creating the central index;
vi) future human resource needs in DND, CSIS and other departments for the subject interviews, perhaps offset by savings in (i) above.

55. Departments will be held to existing resource levels, unless additional allocations are approved by TB. Preparation of detailed directives and guidelines for both the classification and personnel screening policies by TB may involve the creation of small working groups.

CONCLUSIONS

56. There is an urgent need for a more rational personnel security screening policy and an up-to-date classification policy. Clear criteria for identifying positions requiring a security clearance of the incumbent are needed. With the CSIS Act creating an external redress process (SIRC), monitoring of implementation and management by a central agency, and consistent application of reasonable position designation and classification criteria, officials believe the proposals represent a significant improvement and that there will be an established system with integrity that can face the challenge of the most critical external review.

57. There is some expectation that the application of the criteria may result in a net reduction in clearance requests. It must be borne in mind, however, that there has already been some reduction in the number of security screenings conducted by CSIS (53,308 in 1984 versus 74,386 in 1983), perhaps as a result of a former Solicitor General writing to departments asking them to reduce the number of clearance requests to only those necessary and also as a result of CSIS questioning departments on doubtful requests for screening.

58. It is therefore concluded that:

(a) TB should be authorized to issue and amend Operational Policies, directives and guidelines for Security of Personnel and Protection of Government of Canada National Interest Assets in accordance with the recommendations and proposals in this Memorandum;

(b) the Treasury Board and Public Service Commission should examine and prescribe a system of verification for trustworthiness and essential suitability of all public service employees as required by the nature of their duties;

(c) this personnel security policy should apply to all government and non-government personnel whose duties may afford an opportunity to cause injury to the safety and integrity of Canada, except for such cases as O-i-C appointees;

(d) criteria for three security clearance levels and appropriate screening procedures should be established;

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

(i) they are engaged in or may engage in activities which constitute a "threat to the security of Canada" as that term is defined in the CSIS Act;

(ii) because of features of character, or association with persons or groups referred to in (i) above, or through 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 such a way as to constitute a "threat to the security of Canada", as defined.

(f) a security classification system should be authorized for the protection of National Interest information with appropriate designators and injury tests;

(g) TB should be authorized to develop procedures for the safeguarding of other categories of sensitive, non-security, information for later consideration;

(h) the ultimate responsibility of deputy heads for security in their government institutions should be confirmed;

(i) practices should be adopted for the classification of material assets, the control of classification and declassification, and fingerprint records for private sector employees, that a central index of security clearances should be established and that indoctrination certificates and non-disclosure agreements should be reviewed, in view of developing effective non-disclosure agreements.