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

EXECUTIVE SUMMARY

CURRENT SITUATION	ISSUE	PROPOSAL
	I PERSONNEL SECURITY	
1. There is inconsistency and inadequacies in the investigation of the suitability and trustworthiness of prospective employees by personnel managers in many departments and agencies of government.	1. As a result of these inconsistent and inadequate personnel management practices, the security screening system is often misused as a substitute for the basic reference checks for suitability and trustworthiness verification.	1. Policies should be considered and developed by the TB and PSC to strengthen those aspects of the staffing process relating to the assessment of a person's general suitability and trustworthiness, thus obviating the improper use of security screening (M.C., paras. 10-12).
2. CD 35 provides that security screening shall only be employed for persons whose positions afford access to classified information (itself not defined).	2. Some persons hold positions which do not afford access to classified material, but, for reasons relating to the particular nature of the work, afford an opportunity for an incumbent to cause injury to the integrity and security of the state through proximity to people, places, property or information relating to such interests.	2. New personnel security screening policies should apply to those persons occupying government positions, whose positions may afford an opportunity for an incumbent to cause injury to the national interest because of access or proximity to people, places, property or information relating to such interests (M.C., paras 13-15).
3. CD 35 only requires that a person have a Top Secret, Secret or Confidential security clearance if he is to have access to, respectively, material classified as Top Secret, Secret or Confidential.	3. CD 35 does not adequately address what level of clearance is required to ensure the protection of the State's interest.	3. 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:

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

CURRENT SITUATION	ISSUE	PROPOSAL
		- 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 (M.C., paras. 17-22).
4. CD 35 provides two sets of screening procedures for three security clearance levels, rendering the Confidential and Secret clearances the same.	4. The lack of distinction between Confidential and Secret clearances leads to over-screening and to misuse of the full field investigation through requests for Top Secret clearances. An additional cost-effective and valuable technique is not currently mandated.	4. Distinct screening procedures, providing a better basis for the preparation of reasoned security assessments by CSIS and thus deputy heads' decisions to grant or deny clearances at levels in accordance with distinct security requirements, should be available for each of the three clearance levels. In ascending order, the proposals are:

* 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.

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

CURRENT SITUATION	ISSUE	PROPOSAL
		LEVEL I - subversive indices check; - review of irregular information from suitability checks; - credit checks; - subject interviews (new technique) for cause only; - field investigation for cause only; - criminal records check. LEVEL II - same as LEVEL I, except subject interview mandatory. LEVEL III - same as LEVEL II, except field investigation also mandatory. The subject interview has been found to be a highly effective technique in other jurisdictions (M.C., paras. 23-25).
5. CD 35 requires denial of a security clearance on grounds of loyalty considerations to members of communist or fascist parties or affiliated organizations, persons who by word or action support the same or front groups, persons who are secret agents for a foreign power or support such agents, or persons who support	5. CD 35 is rooted in Cold War concerns with communism and fascism. This is too narrow and does not reflect the contemporary threats. It is not in accord with the CSIS Act definition of "threats to the security of Canada". The McDonald Commission argued that the loyalty rejection criteria should be related to the threats	5. The loyalty criteria should relate to threats to the security of Canada. There must be an objective assessment of reliability factors to identify a possible connection with a "threat to the security of Canada" and to determine if these factors exert such influence as to make the person act disloyally. Such a position

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

CURRENT SITUATION	ISSUE	PROPOSAL
organizations advocating or using force to alter the form of government. CD 35 also requires denial of a security clearance on grounds of reliability considerations to persons who are unreliable due to features of character which may lead to indiscretion, dishonesty or vulnerability to blackmail, persons with family or other close relationships with persons described under the loyalty considerations that might make it likely that they be induced to act in a manner prejudicial to Canada's interests, or persons bound by close ties of blood or affection to persons living in foreign countries as may cause them to be subject to intolerable pressures.	defined by Parliament in the statutory mandate of CSIS. The reliability criteria lack, in the main, any causal connection to the risk factors threatening national security.	seems to be in total conformity with the definition of "security assessment" in the CSIS Act (M.C., paras. 26-28).
6. CD 35 has a range, rather than a single standard, of evidentiary standards for rejection depending on the criteria.	6. Should there by a single standard and what should it be?	6. 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;

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

CURRENT SITUATION	ISSUE	PROPOSAL
		(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. (M.C., paras. 29-31; an alternative proposal is set forth in paras. 30 and 31.)
7. Existing policy on separatist activity, as it relates to security clearance, is ambiguous. It is not mentioned in CD 35. A 1976 Cabinet Decision says it is a factor to be reported on in security screening.	7. Should a clear position on separatist activity be adopted? Arguments by McDonald suggest it is not a threat to the security of Canada, per se.	7. The 1976 Cabinet Decision should 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, however, information concerning separatist activities or support that do not relate to a threat to the security of Canada may 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

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

CURRENT SITUATION	ISSUE	PROPOSAL
		provided or is obtained during 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. (M.C., paras. 32 and 33.)
	II PROTECTION OF ASSETS	
8. "Security of Information - 1956" prospectively requires that most government information be security classified.	8. The current system fails to distinguish between information of a private and personal nature and information relating to the security of the state. This had led to misuse of the security classification system to protect sensitive, non-national security information and, thus to misuse	8. A defined National Interest category with appropriate designations is proposed for information and material assets relating to the security of the state to eliminate misuse of the classification system. Other sensitive material of a non-national security character,

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

CURRENT SITUATION	ISSUE	PROPOSAL
	of security screening. A wasteful use of physical and human resources also results.	would be afforded protection under policies to be issued by Treasury Board. (M.C., paras. 34-42.)
	MANAGEMENT OF ADMINISTRATIVE SECUR	
9. No single accountable responsibility centre exists presently for the management of administrative security within the Government of Canada.	9. Should a single agency be designated as responsible for administrative security? Current security policies, directives and guidelines of the Government of Canada are outdated, fragmented and inconsistent.	9. Treasury Board should be authorized to assume a Government-wide management responsibility, through the issuance of the Operational Policies and amendments thereto, and of the detailed implementation procedures in the form of directives and guidelines in the Administrative and Personnel Policy Manuals. These should eventually cover administration of security; personnel security; physical security; communications-electronics security; electronic data processing security; and technical intrusion security. (M.C., para. 45.)