

1. Are current personnel practices for basic reference checking of prospective employees adequate?

Current

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.

Proposal

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. 31-33).

2. Who should be subject to security screening?

Current

CD 35 provides that security screening shall only be employed for persons whose positions afford access to classified information (itself not defined).

Proposal

New personnel security policies should apply to those persons occupying positions, whose duties may afford an opportunity for an incumbent to cause injury through access to information classified in the National Interest (M.C., paras. 34-36).

3. What should determine the required level of security clearance for a person?

Current

CD 35 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 (undefined).

Proposal

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 through access to information classified in the National Interest* (MC., paras. 37-40).

***Note:** Information classified in the National Interest (MC., Annex VII) includes:

- international affairs;
- federal/provincial affairs;
- economic interests;
- confidences of the Queen's Privy Council;
- national security; and
- national defence.

4. What screening procedures should be applied to the various security screening levels?

Current

CD 35 provides two sets of screening procedures for three security clearance levels, rendering the Confidential and Secret clearances the same.

Proposal

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:

LEVEL I (Confidential)

- subversive indices check;
- review of irregular information from suitability check;
- credit checks;
- subject interview for cause only;
- field investigation for cause only;
- criminal records check.

LEVEL II (Secret)

- same as LEVEL I, except subject interview mandatory.

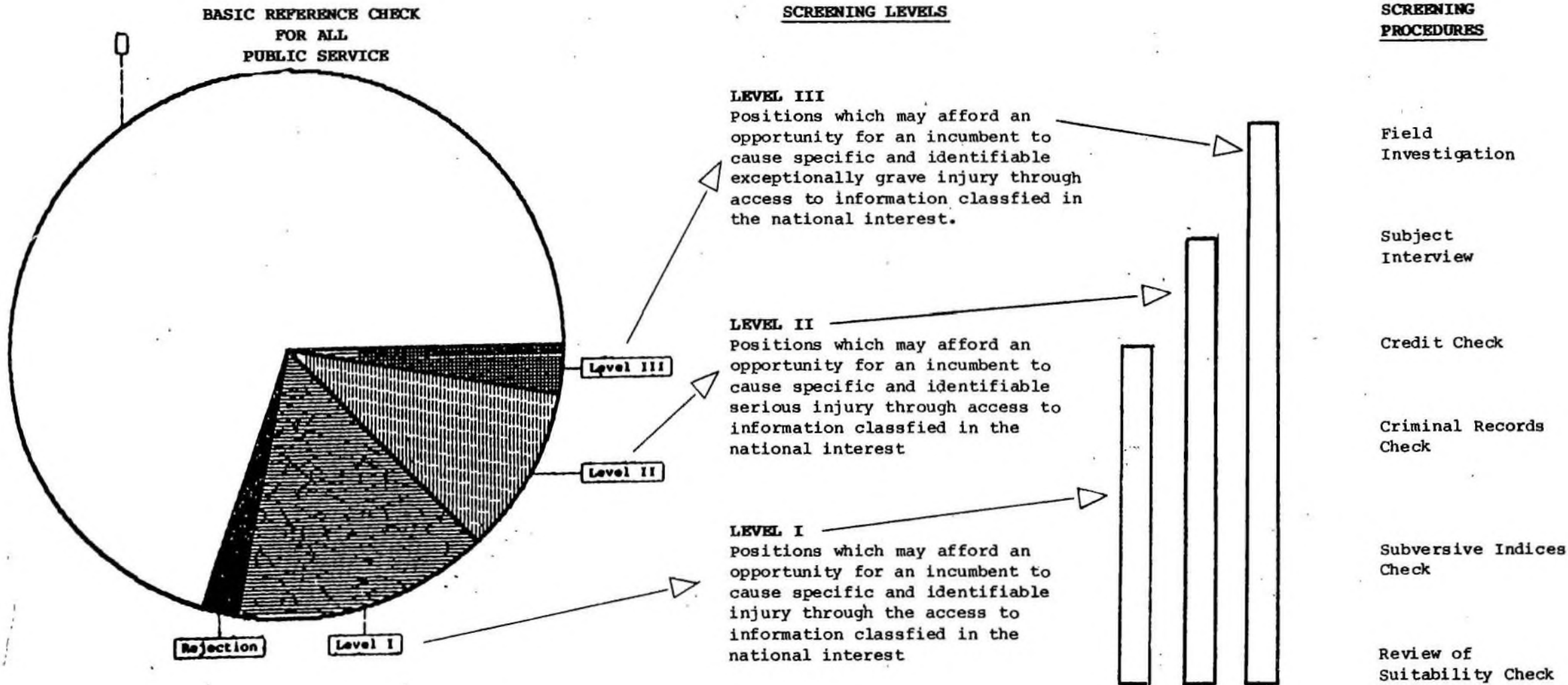
LEVEL III (Top Secret)

- 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. 43-45 and Annex I).

PERSONNEL SECURITY



5. What should be the evidentiary standards and test for denial of a security clearance?

Current

CD 35 has a range, rather than a single test, of evidentiary tests for rejection depending on the criteria.

Proposal

Persons should be denied a security clearance if there are reasonable grounds to believe that there is a possibility ("may") that they have been, are, or will be disloyal. Thus, the evidentiary test proposed is as follows:

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; or
- (b) 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 foreign countries:
 - i) 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; or
 - ii) 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.

(M.C., para 47-50).

6. What should be the appropriate loyalty rejection criteria for employees?

Current

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 organizations advocating or using force to alter the form of government.

Proposed

The loyalty rejection criteria should relate to "threats to the security of Canada", as defined in the CSIS Act. In summary these are:

- espionage or sabotage;
- foreign influenced activities detrimental to Canadian interests;
- terrorism;
- covert or violent domestic subversion;

but do not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the above.

(MC. paras. 51-53 and Annex III).

A0052939_7-003880

7. What should be the appropriate reliability rejection criteria for employees?

Current

CD 35 states that "a person may be unreliable for a number of reasons that do not relate to loyalty".

Unless the risk involved appears to be justified in the circumstances, CD 35 requires the denial of a security clearance 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 interest; 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.

Proposal

Because the CSIS Act defines a "security assessment" as an "appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual" there must be: an identifiable connection between any reliability rejection criteria and actual or possible disloyalty; and an appraisal of how this unreliability factor induces, or may induce a person to act disloyally.

Consequently it is proposed that an objective assessment of an individual's reliability as an aspect of loyalty be made on the following criteria:

- a) personal beliefs
- b) features of character
- c) association with persons or groups considered a security threat; or
- d) family or other close ties of affection to persons living in oppressive or hostile foreign countries.

(M.C. paras. 54-58).

8. What should be the policy position on separatist activity?

Current

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.

Proposal

The 1976 Cabinet Decision is redundant and should be declared 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 (M.C., para 59-60).

9. What should be the security classification system for government information assets?

Current

1. In "Security of Information 1956", there is no definition of what is considered to be government documentation requiring classification.
2. There is no consistent or common criterion governing the injury test designators (i.e. "Confidential", "Secret", "Top Secret").
3. In the use of the designator "Confidential" there is combined, injury to the state (a security criterion) with injury to an individual (a privacy criterion).
4. "Restricted" as a designator does not relate to injury to the state for national security purposes and therefore a non-security classification is included in the security classification system.

(M.C., Annex V, copy attached)

Proposal

1. A new specific definition is proposed for all government information to be classified for security reasons as being in the "National Interest". This definition will only include government information in the following categories: international affairs; federal/provincial affairs; economic interests; confidences of the Queen's Privy Council; national security; and national defence (M.C., Annex VII).
2. Using the same designators as before, a three level classification system with a common test of injury is proposed, as follows:

When unauthorized disclosure, destruction, removal, modification or interruption of government information could reasonably be expected to cause:

- exceptional grave injury [Top Secret];
- serious injury [Secret]; or
- injury [Confidential];

to the National Interest of Canada.

(M.C., para. 66)

3. The definition proposed for the designator "Confidential" relates only to injury to the state. Sensitive "personal information", whose unauthorized disclosure might harm individuals, is to be protected by Treasury Board through a separate administrative procedure.
4. It is proposed that "Restricted" be dropped as a security designator, because by definition no injury to the national interest is involved.

(MC, Annex VI and VII, copy attached)