D R A F T

MEMORANDUM TO DEPUTY MINISTERS

INTERIM GUIDELINES ON SECURITY CLEARANCE

[F on file at SAC-2/78
Chantt BC fls

OBJECT

1. To set out interim guidelines governing the personnel security clearance program.

BACKGROUND

2. More than fifteen years have passed since the principal document on personnel security clearance policy (Cabinet Directive #35, Security in the Public Service of Canada, December 18th, 1963) was written.

3. Since 1963 the Public Service has undergone tremendous growth, the public attitude toward security questions has changed, legislation on individual access to personal information has been enacted, legislation on freedom of information is possible and, most importantly, the nature of the government interests requiring protection through such policy has also changed. Resulting from these changes Cabinet Directive #35 has become obsolescent.

4. Recognizing the need to replace CD#35 with a more comprehensive policy document on security clearances, officials have prepared a draft document dealing with the subject, but because of its complexities and direct relationship to other policy documents under Cabinet consideration, it is doubtful that it will receive early approval.

5. Notwithstanding changes which have occurred with the passage of time, the fundamental principle that the government can repose confidence both in the loyalty and reliability of individuals appointed to carry out its business, must be upheld. To effect this it is necessary to recognize that security interests of the government must be considered not only in relation to information, but also to materiel, personnel and services.

6. For the purposes of these guidelines, policy and procedures related to the security clearance of personnel will be principally dealt with in relation to sensitivity of information related to national security and non-national security.

NATIONAL SECURITY

Areas For Protection

7. Personnel security clearance policy in respect of national security matters relates to the control of access to national security information. Where materiel of a national security interest is involved the protection of the national security classification system is deemed to extend to information about such materiel.

8. Information relating to national security is deemed to include the following categories:

a. International relations;

b. National defence;

c. National security;

d. National federal-provincial relations;

e. Confidences of the Queen's Privy Council; and

f. Activities by national investigative bodies in relation to;

(1) national security,

(2) detection and suppression of crime generally, or

(3) investigations pertaining to the administration or enforcement of any Act of Parliament

9. Matters of international relations, national defence and national security will include the product of foreign intelligence gathering, the methods used for gathering foreign intelligence, and the sources used.

10. Information in the national security system will be classified according to the degree of sensitivity appropriate to the classification levels hereunder:

a. TOP SECRET - only when unauthorized disclosure, removal, modification or destruction could cause exceptionally grave damage to national security;

b. SECRET - only when unauthorized disclosure, removal, modification or destruction could cause serious damage to national security;

c. CONFIDENTIAL - only when unauthorized disclosure, removal, modification or destruction could be prejudicial to national security; and

d. RESTRICTED - only when unauthorized disclosure, removal, modification or destruction could be undesirable to national security.

Policy

11. The national security classification system and related personnel security clearance procedures for access to such information are conservative instruments. Their development and application is designed to prevent access, not allow it. The interest of their application in the Federal context is at two levels:

a. To deny all access by the public at large to national security information; and

b. to deny access to the vast majority of Federal public servants to the same material.

12. The government has a responsibility to ensure the LOYALTY and RELIABILITY of persons in positions requiring access to national security information. Persons who are to be granted such access will complete a copy of the Personnel Security Clearance Questionnaire (see Annex A) and be fingerprinted.

13. The National Security Agency (RCMPolice Security Service and Criminal Investigation Branch) will cause a check to be made of subversive and criminal indices and, where access to TOP SECRET information is required, will conduct a field investigation.

Implementation

14. All persons of the rank of Director (SX1) or above will be security cleared to the TOP SECRET level. The Deputy Head will also identify all other positions in his department, the incumbents of which require access to TOP SECRET information. A list of these persons will be submitted by each department or agency to the National Security Agency. Additions to the list must be justified, and deletions from the list must be notified to the National Security Agency.

15. Other departmental employees requiring access to national security information below the TOP SECRET level will be security cleared to the level determined by the Deputy Head.

Rejection Criteria

16. A personnel security clearance must not be granted to a person:

a. whose LOYALTY is in doubt because there are reasonable grounds to believe the person:

(1) is or has engaged in or is planning to engage in, or

(2) is or has been a member of an organization or, by his/her words or actions, supports or supported an organization engaged in or planning to engage in:

(a) acts of espionage or sabotage;

(b) activities directed toward gathering intelligence relating to and contrary to the best interests of Canada;

(c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;

(d) activities directed toward actual or potential attack or other hostile acts against Canada;

(e) activities directed toward the commission of terrorist acts in or against Canada;

(f) activities of a kind which are detrimental to Canada because of such factors as a commitment to an ideology, a cause, a movement, a foreign government, or an economic interest;

(g) activities directed toward the creation of civil disorder in relation to any of the activities referred to in sections (a) to (f) above; and/or

b. whose RELIABILITY is in doubt because the person may be indiscreet or vulnerable to blackmail or coercion in respect to his/her access to national security information as a result of:

(1) features of character such as those relating to greed, indebtedness, sexual behaviour, alcohol or drug abuse, mental instability or criminal activity; or

(2) family or other close relationship with

(a) persons who are persons as described in a. above, or

(b) persons who are living in countries whose governments may use such relationship for purposes prejudicial to the safety or security of Canada;

unless, after careful consideration of the circumstances, including the value of the person's services, the risk involved seems justified in the opinion of the deputy head.

NON-NATIONAL (CIVIL) SECURITY

Areas for Protection

17. Personnel security clearance policy requiring access clearance will relate not only to access to non-national security sensitive information, but also the handling of other valuable government assets.

18. For purposes of identification non-national (civil) security information and materiel requiring access clearance is deemed to relate to one or more of the following:

a. Personal privacy;

b. Judicial issues under the Inquiries Act;

c. Legal considerations;

d. Prohibitions established by Federal enactments;

e. Commercial or proprietary considerations, and

f. Decision-making processes respecting preparation of legislation and conduct of parliamentary business.

19. Information and materiel in the non-national (civil) security system will be designated according to the degree of sensitivity or value appropriate to the classification levels hereunder:

PROTECTED - Personnel

PROTECTED - Financial

PROTECTED - Legal

PROTECTED - Corporate

PROTECTED - Privileged

Policy

20. The reliability of persons must be established when their duties relate to the following:

a. Cash and Negotiables - day-to-day handling of significant amounts of cash or negotiables, or immediate access to financial records or programmes whereby theft or conversion of funds may be achieved by alteration or deletion;

b. Valuable Assets - day-to-day access to such valuable assets as paintings, manuscripts, antiquities, etc.;

c. Valuable Information - frequent access to such valuable information as future plans involving expenditures of public funds, contracts, audits, programmes involving change in government policy, patents, research with commercial potential, etc. The principle to recognize in this category is whether there is potential for the information to be stolen, sold or otherwise revealed for significant personal gain;

d. Sensitive Information - frequent access to personal information related to such matters as medical or credit records. The principle to recognize in this category is confidentiality and whether there is potential for the information to be misused;

e. Contractual arrangements - direct involvement with the actual procurement of goods and services from commercial companies to the extent that the potential exists for significant personal gain;

f. Corrections and Parole - direct contact on a day-to-day basis with offenders;

g. Drugs - access to and handling of drugs; and

h. Government - access to government plans, decisions, documents etc. which are not subject to National Security protective safeguards.

21. Persons who are to be granted access to non-national (civil) security information or material will complete a copy of the Short Personal History Form (see Annex B) and be fingerprinted.

22. RCMP CIB will cause a check to be made of criminal indices. Reference checks based on other information provided in the Short Personal History Form will be done by the responsible staffing officer.

Rejection Criteria

23. A personnel security clearance must not be granted to persons whose RELIABILITY is in doubt when features of character may make them unfit to perform their duties in a trustworthy manner. Such impediments might include continuing,

a. criminal activity;

b. drug and/or alcohol abuse; and

c. personal-related problems which may become apparent during staffing action.

Application

24. The granting of a security clearance for access to non-national (civil) security information or materiel will be at the discretion of the Deputy Head concerned.

Implementation

25. The Deputy Head will identify all positions within his department or agency whose incumbents require access to non-national (civil) security information or materiel.

ALL OTHER POSITIONS

26. All positions other than those requiring one of the two forms of access clearance will be annotated in such a way that the incumbent will be subject to a form of RELIABILITY check made by the responsible staffing officer on completion of the Short Personal History Form at Annex C.

27. The distinction between reliability checks made in this context and those made for access to information or materiel is that no criminal indices check is required and suitability will rest only on a mandatory check of personal references provided at the time of employment application.

CONTRACT/INDUSTRIAL EMPLOYEES

28. Where contract/industrial employees require access to carry out activities on behalf of the federal government equivalent to those in the three classes identified, the same standard of clearance demanded of public servants will be required.

CONCLUSIONS

29. It is recognized the implementation of these personnel security guidelines may cause initial difficulty primarily related to the identification of positions requiring action beyond simple departmental staffing initiatives. Nonetheless, beyond such an initial phase of relative dislocation the introduction of these measures will regularize the degree of confidence which the government must have in respect of access to sensitive areas of its operations.

30. Clearly, the introduction of these measures will limit the requirement for clearance procedures to a very small percentage of the public service complement and the resultant simplification will, over time, make much easier the control of access to areas requiring protection.

31. Equally, and importantly, these measures are intended to satisfy concerns which have been expressed in the forum of labour/management relations in the public service.