Commission of Inquiry
Concerning Certain Activities of the
Royal Canadian Mounted Police

Second Report — Volume 2

Freedom and Security under the Law

August, 1981

Commission of Inquiry
Concerning Certain Activities of the
Royal Canadian Mounted Police

Second Report — Volume 2

Freedom and Security under the Law

August, 1981

FREEDOM AND SECURITY UNDER THE LAW

ADNP

COMMISSION OF INQUIRY
CONCERNING CERTAIN ACTIVITIES OF THE
ROYAL CANADIAN MOUNTED POLICE

Second Report — Volume 2

FREEDOM AND SECURITY UNDER THE LAW

August, 1981

Available in Canada through

Authorized Bookstore Agents
and other bookstores

or by mail from

Canadian Government Publishing Centre
Supply and Services Canada
Ottawa, Canada, K1A 0S9

Catalogue No. CP32-37/1981-2-2E
ISBN 0-660-10952-2
ISBN 0-660-10950-6 (V. 1 and 2)

Canada: $12.00 (2 Volumes)
Other Countries: $14.40 (2 Volumes)

Price subject to change without notice

PART VI

A PLAN FOR THE FUTURE: MANAGEMENT, PERSONNEL, AND STRUCTURE OF A SECURITY INTELLIGENCE AGENCY

INTRODUCTION

INTRODUCTION

1. Having concluded that Canada needs a security intelligence organization at the federal level, and having decided on the basic functions of this organization, we are now in a position to discuss two difficult and related issues: first, the management and personnel practices of a security intelligence organization and, second, its appropriate structure within the Canadian government.

2. The first issue demands our consideration of the following questions:

> What overall approach to management is most likely to produce effectiveness and encourage behaviour which is both legal and proper?
>
> What should be the role of the Director General and the organization's senior management? What qualities should they possess?
>
> What kinds of people should this organization attract and how should they be recruited, trained, supervised, and rewarded?
>
> What procedures are appropriate to govern such areas as internal security, discipline, and complaints?

Our answers to these questions will lead logically to a discussion of the second issue, that of appropriate structure. In that regard, we shall tackle one of the most complex questions facing our Commission: should the security intelligence organization remain part of the R.C.M.P., or should it, or at least part of it, be separated from the Force? And if separation appears preferable, should a security intelligence organization be a separate department of the federal government, part of an existing department, or an agency with a distinct set of relationships to the central management bodies of the Federal Government — the Treasury Board, the Public Service Commission and the Privy Council Office?

3. These management, personnel and structural issues have a long history. Indeed, as we shall illustrate in the next chapter, R.C.M.P. senior management and, to a lesser extent, Ministers and other senior officials within the Federal Government, have been wrestling with these problems for at least 25 years.

CHAPTER 1

THE HISTORICAL CONTEXT

4. Our objective in this chapter is to describe how management and structure have been dealt with in the past — the major studies, the recommendations which these studies made, and the impact they had on the R.C.M.P. Security Service. We end this chapter by summarizing briefly the major conclusions we have reached on these issues.

A. POST WORLD WAR II TO THE ROYAL COMMISSION ON SECURITY, 1968

5. As we noted in Part II, Chapter 2, which traces the history of the Security Service, its management and structure developed along a relatively stable pattern in the three decades following World War II. A large increase in staff during this period accompanied a series of organizational changes. These changes had the dual effect of enhancing the status of the security intelligence function, as well as giving it an organizational form which became increasingly separate from the criminal investigation side of the Force. There were also a number of changes which were premised on the specialized needs of security intelligence — for example, the hiring of civilians in research and analytical capacities, and the development of training courses on security intelligence matters. Two internal studies, one by Superintendent Rivett-Carnac in 1947 and another by Assistant Commissioner Harvison in 1956 (both of whom became Commissioners), were instrumental in pointing the Force in these directions.

6. There was, in addition, a third internal study of the Force's security intelligence function, completed in 1955. This study put forward recommendations which broke sharply with the relatively stable development pattern we described above. Its author was a civilian member employed by the R.C.M.P. in a senior research capacity, who was asked by Commissioner Nicholson for proposals as to the most effective use of civilians in the Special Branch.[1] Interpreting this request broadly, the Report called for a radical reorganization of the security intelligence function. The major recommendation was for the establishment of a "two team organization" comprised of a Special Branch under a Deputy Commissioner and a parallel Internal Security Service (ISS) under a Director with the equivalent rank of a Deputy Commissioner. Both the

[1] Special Branch was the name then given by the R.C.M.P. to the organizational unit responsible for the security intelligence function. For a description of how the name of the Security Service evolved, see Part II, Chapter 2 of this Report.

Deputy Commissioner and Director would report to the Commissioner of the R.C.M.P. The ISS would be fully civilian in nature, with complete responsibility for counter-espionage, research, policy development, and foreign liaison. It would share responsibility with the Special Branch (each would have complementing "specialties") in the following areas:

— counter-subversion

— security screening

— governmental and public liaison

— emergency planning

In counter-subversion, for example, the Special Branch would do the day-to-day "detailed coverage" activities, while ISS would "select from this coverage those cases requiring long term specialized attention". In a summing up analogy, the Report compared the Special Branch to an army, with its high visibility and systematic activities performed across Canada; the ISS, on the other hand, would be more like a guerrilla force, covert in nature, and capable of concentrated sudden strikes against specific targets.

7. The Report preferred this two-team approach to an upgraded Special Branch for two reasons. First, it judged that the Special Branch was not doing its job, and, given the likelihood of an increasingly dangerous international environment (the Report was written at the height of the Cold War), the Special Branch did not have the time required to shore up its weaknesses. Second, a police force could not perform the duties of a fully specialized security service. For example, recruiting, training, and career planning practices of police forces were inappropriate, the author said, for a security service which required professionals from a broad range of disciplines, with a sophisticated understanding of revolutionary processes.

8. That the R.C.M.P. did not implement those recommendations was not surprising. Two R.C.M.P. historians, Carl Betke and S.W. Horrall, summed up the Force response this way: "Not surprisingly, that comprehensive advice from a civilian newcomer of no operational experience was rejected". In our view, the rejection of some of the recommendations was justified. But it was unfortunate that the Force and the government took little or no action to deal with other issues raised in the Report, including the following:

— whether or not police recruiting, training, and staffing procedures are appropriate for a security service;

— the differences between the role of a police force and that of a security service;

— the necessity for legal advice as a component of security service decision-making;

— the question of whether or not a security service is required to do illegal or improper acts and the problems this dilemma created for its members;

— the capabilities required of a security service for policy development and governmental liaison;

— the need for a legislative charter for the security intelligence function.

9. As we shall see, these issues would return to haunt the R.C.M.P., and indeed are still current today.

B. THE ROYAL COMMISSION ON SECURITY, 1968, AND ITS AFTERMATH

10. The Royal Commission on Security, chaired by Mr. Maxwell Mackenzie, completed its report in 1968.[2] Of relevance to this chapter was the Commission's recommendation calling for "the establishment of a new civilian non-police agency to perform the functions of a security service in Canada."[3] The Commissioners based this recommendation on three arguments:

(i) The differences between police and security duties are wide. Consequently, a security service should not orient its recruiting and training practices, its career patterns and its organizational structures towards the requirements of a police force.

(ii) The R.C.M.P. had failed to play an effective role in taking "desirable initiatives", or in stating the case for necessary security measures at high level policy-making forums within the federal government.

(iii) The association of the security function with the police role tended to make the work of both the Security Service and the rest of the R.C.M.P. more difficult. On the one hand, inquiries made by civilians in connection with security clearances would be received with more understanding than would similar inquiries made by policemen. On the other hand, it is not appropriate for a police force to be concerned with activities that are not crimes or suspected crimes. Moreover, a security service might be involved in actions "... that may contravene the spirit if not the letter of the law"[4] and that may infringe on individuals' rights. Such activities are not appropriate police functions.

11. From our study of R.C.M.P. file material, we know that the reaction of R.C.M.P. senior officers to this recommendation was one of shock and disbelief. For example, Assistant Commissioner W.L. Higgitt, who at the time was the officer in charge of the Security and Intelligence Directorate and became Commissioner in the following year, in an address to the Security Panel (a senior interdepartmental committee of officials), termed the recommendation for a separate civilian service "a travesty of justice," and added that "the Soviet Intelligence would be jubilant. They could never hope to duplicate the accomplishment".

12. Once the initial shock had subsided, the senior management of the R.C.M.P. put together a detailed rebuttal of the Royal Commission's Report. The Force's critique was threefold. First, the Royal Commission had done its job poorly: it had failed to assess the effectiveness of the Security Service, had

---

[2] For a description of the events leading up to the establishment of the Royal Commission on Security, see Part II, Chapter 2 of this Report.

[3] *Report of the Royal Commission on Security*, paragraph 297.

[4] *Ibid.*, paragraph 57.

made numerous errors in fact, had ignored other areas of importance, and had not taken into account evidence supplied by the R.C.M.P. Second, creating a separate security service would be a serious mistake, in the Force's view, for the following reasons:

— a new civilian agency would be easily penetrated;

— the advice was, where possible, to establish a security service as part of the national police;

— only the R.C.M.P. was spread sufficiently widely across Canada to constitute an adequate service;

— the R.C.M.P. had built up meaningful liaison with foreign agencies and these relationships could not be readily developed by a new service.

Finally, if the recommendations concerning the Security Service were ever to be published, the Force believed that severe damage would result to the Canadian security community.

13. The documents relating to the treatment of the Report by the Cabinet Committee on Security and Intelligence and its various committees of officials indicate that much of the consideration focussed on the question of whether or not to publish even an abridged version of the Report. There appeared to be little support, either at the ministerial or the official level, for the new civilian agency proposed by the Royal Commission.

Prime Minister Trudeau's 1969 Statement

14. After a lengthy debate, the Cabinet Committee on Security and Intelligence agreed to publish an abridged version of the Royal Commission's Report. In tabling the Report in the House of Commons on June 26, 1969, the Prime Minister rejected the Commissioners' recommendation for a separate security service and announced, instead, that the security intelligence function would remain within the Force but become ". . . increasingly separate in structure and civilian in nature". The following are the key paragraphs in which Mr. Trudeau outlined this new policy:

> After careful study of the considerations put forward by the commissioners in support of their recommendation, we have come to the conclusion that current and foreseeable security problems in Canada can be better dealt with within the R.C.M.P. through appropriate modifications in their existing structure than by attempting to create a wholly new and separate service.
>
> We are keenly aware that the R.C.M.P. are one of the most honoured and respected of Canadian institutions. The force has come to be recognized as one of the finest national police forces in the world, whose members, as the commissioners rightly state, are "carefully selected, highly motivated, and of great integrity." The government also recognizes that no organization is perfect, and that there is some validity in the view of the royal commissioners that some basic differences do exist between police and security duties, by their very nature.
>
> It is therefore the government's intention, with the full understanding of the R.C.M.P., to ensure that the Directorate of Security and Intelligence

will grow and develop as a distinct and identifiable element within the basic structure of the force, and will be more responsive, in its composition and character, to the national security requirements described by the commissioners. The basic aim will be to develop the security service so as to draw on the police services for personnel of suitable qualifications and character, and to retain administrative, research, documentation and other services in common with them. The security service, under the Commissioner of the R.C.M.P., will be increasingly separate in structure and civilian in nature.

New and more flexible policies in relation to recruiting, training, career planning and operations will be calculated to ensure that Canada's security service will be capable of dealing fairly and effectively with the new and complex security problems which we will undoubtedly face in the future, and also to ensure that it clearly reflects the nature of our cultural heritage. Under the new arrangements it will be possible, for example, for an increasing number of university graduates from all parts of Canada to join the Directorate in a civilian capacity and to aspire to positions at the top of that organization, thereby making the kind of contribution referred to by the commissioners. Nothing in the proposed changes will unfairly prejudice the career expectations of people already in the service.[5]

15. The Prime Minister's statement was, in essence, a compromise. What Mr. Trudeau was attempting to achieve was a Security Service similar to the one envisioned by the Royal Commission, but located within the R.C.M.P. The statement made no mention of any implementation scheme.

16. In replying to Mr. Trudeau's statement, both the Honourable Robert Stanfield, the Leader of the Opposition, and Mr. T.C. Douglas, Leader of the New Democratic Party, expressed reservations about the government's decision not to form a civilian non-police agency. Mr. Stanfield wondered "... whether the mounted police, as it is presently constituted and organized, lends itself very readily to the sort of modifications to which the Prime Minister refers." He went on to add:

> My initial reaction might be that we are more interested in considering the proposal for a special agency, though I can see certain difficulties in this regard. But I look forward to hearing a further explanation in the house by the government when we have our discussion, presumably in the fall.[6]

Mr. Douglas based his support for a separate agency on what he believed to be "... a difference in the type of training required, the form of recruitment and the structure of a police force on the one hand, and a security agency on the other."[7]

17. After a thorough study of relevant R.C.M.P. files, and after questioning numerous witnesses including Ministers and senior officials on this topic, we conclude that the R.C.M.P. has not sufficiently implemented the policy announced by the Prime Minister in his 1969 statement, nor has it made a concerted effort to do so. For the better part of the last decade, the successive Commissioners of the Force and their senior managers who were not part of

---

[5] House of Commons, *Debates*, June 26, 1969, pp. 10636-10637.

[6] *Ibid.*, p. 10639.

[7] *Ibid.*, p. 10640.

the Security Service have endeavoured to ignore the policy statement whenever possible. When circumstances forced them to deal with the statement, they have tended to misinterpret it by concentrating on the "increasingly separate in structure" aspect of the policy, showing insufficient concern for what has come to be called "civilianization" of the Security Service. A careful reading of the Prime Minister's statement reveals that increasing separation was only a means to achieving more flexible personnel policies so as to facilitate civilians' joining the Service and rising to senior positions. The Prime Minister, as we shall see later in this chapter, made this abundantly clear to the Force several years later.

18. The use of appropriate statistics is one way of assessing what has happened to the government's policy since 1969. Before introducing these statistics, we refer again to a basic feature of the R.C.M.P. Security Service which we explained in the introductory chapter of this Report. The Service has four different types of employees:

— public servants, who fill mainly clerical or support staff positions;

— special constables, who perform specialized roles in such areas as security screening;

— civilian members, who were first hired in the early 1950s to perform research analyst roles and who now, in addition, perform specialized functions in translation and in technical areas dealing with computers and sophisticated surveillance technology;

— regular members, who first joined the R.C.M.P. as policemen, and who, after receiving basic training, usually spend several years in regular policing before joining the Security Service.

Since 1969, there have been no substantive changes in the methods of recruiting regular members into the Security Service. They must still train and serve first as police officers. Consequently, to judge the progress in implementing the policy enunciated by the Prime Minister in 1969, we must examine what has happened to the civilian member category of employee.

19. The statistics we have compiled lead to three conclusions. First, the civilian member component within the Security Service has increased in both absolute and relative terms, but it is significantly smaller than the regular member component. Second, civilian members are heavily concentrated in lower ranking jobs. Third, most of the senior positions held by civilians are not in the key operational sectors of the Service but rather, they are in service branches. Moreover, since 1969, there is evidence that there has been a relative decline in the civilian component making up the operational units within the Security Service.

20. The growth in civilian members has been about 125 per cent since 1969. Table 1 illustrates how the civilian component has grown in relative terms.

Table 1

Established Positions As a Percentage of the Total Security Service Strength

	1969	1979	Change
Regular Members	53.3%	46.1%	-7.2%
Special Constables	9.8%	13.2%	3.4%
Civilian Members	9.9%	17.2%	7.3%
Public Servants	27.0%	23.5%	-3.5%
Total	100.0%	100.0%	

In relative terms, the civilian member component as a percentage of the total Security Service has grown from 9.9 per cent to 17.2 per cent. Even with this growth, the civilian member component is still significantly smaller than the regular member component. These figures, if anything, overstate the growth in the civilian member category.

21. Table 2 is the basis for the second conclusion that the large majority of the civilian component is in the lower ranks. To help the reader interpret this Table, we note that civilian members do not have ranks as do regular members. In comparing civilian positions to those of regular members, salary ranges have been used as the basis of comparison. The ranks of regular members are as follows (proceeding from the most junior to the most senior): constable, corporal, sergeant, staff sergeant, inspector, superintendent, chief superintendent, assistant commissioner, deputy commissioner and commissioner. Corporals are called junior non-commissioned officers (Jr. NCOs). Sergeants and staff sergeants are called senior non-commissioned officers (Sr. NCOs) and those with the rank of inspector and above are called officers.

Table 2

Distribution of Regular Members (RMs) Positions and Civilian Members (CMs) Positions By Rank - March, 1980

	Senior Officers	Senior NCOs	Junior NCOs	Constable & lower	Total
RMs who are	9.4%	31.9%	44.3%	14.4%	100%
CMs who are equivalent to	2.4%	28.6%	17.5%	51.5%	100%

22. Finally, Table 3 illustrates that civilian members holding relatively senior ranks within the Service are significant in service sectors but not in operational sectors.

Table 3

Comparison by Rank of Established Positions of Civilian Members and Regular Members - March 1980

A. In Service Sectors: Percentage of Established Positions Held

	Civilian Members	Regular Members	Total
Officers	22.9%	77.1%	100%
Senior NCOs	50.5%	49.5%	100%
Junior NCOs	44.7%	55.3%	100%
Constable & Lower	96.9%	3.1%	100%

B. In Operational Sectors: Percentage of Established Positions Held

	Civilian Members	Regular Members	Total
Officers	1.9%	98.1%	100%
Senior NCOs	5.5%	94.5%	100%
Junior NCOs	4.3%	95.7%	100%
Constable & Lower	36.4%	63.6%	100%

23. The fact that not one civilian member, with the exception of the Director General, now holds an officer-equivalent position with operational responsibilities is perhaps the best single indicator that the type of security service envisioned by Prime Minister Trudeau has not materialized. In particular, this statistic should be looked at in the light of the Prime Minister's statement that "... it will be possible, for example, for an increasing number of university graduates from all parts of Canada to join the Directorate in a civilian capacity and to aspire to positions at the top of that organization, thereby making the contribution referred to by the commissioners." Moreover, there is some evidence to suggest that since 1969 the situation of civilian members in the operational sectors of the Service has actually deteriorated. Table 4 below compares their position in 1968/69 with that of 1977. More up-to-date comparisons are difficult because of at least one organizational change which has removed an operational unit from the Security Service. We have no reason to believe that the situation has improved significantly in the last three years.

Table 4[8]

Percentage of Positions Held by Civilian Members in Operational Sectors by Rank

	1968/69	1977
Officer	8.7%	.0%
Senior NCOs	5.4%	.4%
Junior NCOs	6.8%	1.9%
Constable & Lower	14.1%	25.9%

[8] This Table is slightly adapted from a similar one developed by civilian members in preparing a brief for the Special Committee on the Review of Personnel Management and the Merit Principle, commonly referred to as the D'Avignon Committee. Unlike Tables 1 to 3, this one is not based on established positions, but rather uses actual numbers of people employed at a given point in time.

24. In our discussions with members of the R.C.M.P. about the Prime Minister's 1969 policy statement, many have pointed to the improvement in formal education levels of those within the Service as indicating that the Force has taken the policy statement seriously. Table 5 below demonstrates that formal education levels, especially among regular members, have indeed improved.

Table 5

Percentage of Security Service Employees with University Degrees

	1969	1979
Regular Members	5.5%	21.4%
Civilian Members	13.8%	26.3%
Special Constables	.7	1.6%

25. Several policies have been responsible for producing these changes: sending regular members of the Security Service to university as full-time students; offering reimbursement of tuition fees for part-time university study; and adopting several Force-wide programmes, now discontinued, to encourage university graduates to join the Force. But none of these programmes was really directed at the main objective of the Prime Minister's policy, that is, "for an increasing number of university graduates... to join the Directorate in a *civilian* capacity and to aspire to positions at the top of that organization". (Our emphasis.) Moreover, we believe that there is an important difference between, on the one hand, recruiting people with university backgrounds and, on the other, sending existing members of the Security Service to complete university degrees. We concur with Mr. R.D. French, an associate professor at the Faculty of Management, McGill University. After submitting a brief to this Commission, he had this to say in the question period during the public hearing:

> I would like to observe that the kinds of social experience and breadth of acquaintanceship and catholicity or variety of background, that you find at the University level, and that you experience as a young generally single student, are not comparable to going to University and getting a B. Com. in management or a B.A. in Political Science, or whatever, at the age of thirty or twenty-eight. I think they are fundamentally different things. I think it is highly desirable that R.C.M.P. officers who can benefit from University education get one. That's first class. But it is not a substitute for a broader net at the point of initial recruitment into the organization.
>
> (Vol. 95, pp. 15533-15534.)

26. While there is little evidence of "new and more flexible policies" aimed directly at implementing the June 1969 policy statement, there is evidence in at least one personnel area — classification — of the Force's having adopted policies which point in the opposite direction to that intended by the Prime Minister. The Security Service, along with the rest of the Force, began developing a new classification system in 1971 under the general direction of

the Treasury Board. The new system, which was finally implemented on April 1, 1975, had the important feature of including "police training and experience" as a prerequisite for most of the senior and middle management jobs in the Service and for all officer equivalent jobs in the operational area with the exception of the Director General's position. Including such a prerequisite was not forced on the R.C.M.P. by the Treasury Board. The result of this classification system has been to provide virtually no career path for civilians in the operational side of the Service.[9] For those in the technical services areas of the Service, the most senior job a civilian can assume is at the Superintendent level (Chief Superintendent, Assistant Commissioner and the Director General are three levels above the Superintendent rank.)

27. The adoption of the classification system has also had an unintended effect on the status of civilians within the Service. Until 1975, civilian member salaries were tied to salary levels of regular members. With the adoption of the new classification system, civilian member salaries were tied to equivalent jobs in the Public Service, and did not keep pace with the more rapid rise in police salaries. Thus, civilian positions within the Security Service for the last five years have been gradually downgraded when compared to regular member positions.

28. We should note one recent change to the career paths of civilian analysts within the Service. In 1979, the Security Service created eight additional "dual" staffing positions (such positions can be filled by either regular members or civilians) in certain operational branches at Headquarters. One of these positions is at the inspector level (the first rank in the officer category); five are at the senior NCO level. This change is part of a longer term plan with two objectives: first, to enhance gradually civilian career paths within the Service itself, and second, to provide civilians with government-wide career paths by converting civilian member positions into regular Public Service positions.

29. We view this longer term plan with substantial reservations. It is clear, for example, that civilians within the Service will still remain in basically "support" roles. As the authors of one recent document outlining this new plan put it:

---

[9] The R.C.M.P. is not unique among Canadian police forces in failing to provide meaningful career paths for civilian members in operational areas. In a 1977 report reviewing the Criminal Intelligence Service of Canada — a confederation of major police forces across Canada to provide a co-ordinated approach against organized crime — the authors had this to say:

> 11.6 There was one area in which the views of the members interviewed by both Audit Teams approached unanimity. It was in regard to non-police participation in the intelligence network at any level where they can exert authority or control. Their loyalties, discipline and methods are invariably suspect just by virtue of not being members of the police community. This drains support for the program and undermines confidence in the security and integrity of the system.

> It is questionable whether a command structure which proposes other than regular members in command positions would be accepted. The perception is that it would not make for a smooth functioning situation within the Force.

Thus, the civilian career paths will remain stunted, resulting in the same second-class status that has characterized the civilian component of the Security Service for 25 years. This continuing irritant, coupled with greater mobility within the Public Service, will likely mean that the better civilian analysts will soon leave the Security Service to pursue more promising careers elsewhere. The effectiveness of the Service will suffer accordingly.

30. Statistics and personnel policies, however, do not tell the whole story. To appreciate fully why the 1969 statement was never satisfactorily implemented, we now describe the actions taken, or not taken, by some of the key individuals — the Solicitors General, the Commissioners of the R.C.M.P., the Directors General of the Security Service.

C. THE ERA FOLLOWING THE ROYAL COMMISSION ON SECURITY: 1969-80

The early 1970s

31. The drafts of the Prime Minister's statement to the House of Commons on June 26, 1969, in the preparation of which senior members of the Force participated, contain an early hint about the Force's attitude to what was to be proposed. In the penultimate draft, the government was intending to announce this new direction "... with the full agreement and understanding of the Force..." When Prime Minister Trudeau finally read the statement to the House of Commons, it was only "... with the full understanding of the Force".

32. Even "full understanding" may have been an overstatement. On June 27, 1969, the day following the Prime Minister's statement, Assistant Commissioner Higgitt, who was then the officer in charge of the Security and Intelligence Directorate and who would soon be named the new Commissioner of the R.C.M.P., wrote to his counterparts in foreign security services, enclosing a copy of the Prime Minister's statement and a copy of the abridged report of the Royal Commission on Security. He summed up his reaction to the new policy this way:

> Naturally, we have welcomed this renewed statement of confidence in us and *will now be able to carry on as before* with really only the mildest of organizational adjustments.
>
> (Our emphasis.)

Mr. Higgitt wrote a similar letter to his senior staff in the Security and Intelligence Directorate and included the above sentence unaltered.

33. In testimony before us, Mr. Higgitt has also indicated that he was opposed to the appointment of a civilian from outside the R.C.M.P. as the new Director General of the Security and Intelligence Directorate:

> The change that was then made was that the Director General should become a civilian and a person who had not had the advantage of coming through, of gaining the experience of coming through the Force, and indeed, coming through the Security Service side of the Force. Now, I objected in principle to that . . .and made my objections very well known to those in government circles at the time. But I did not object to the person involved.
>
> (Vol. 84, pp. 13732-13733)

34. The "person involved" was Mr. John Starnes, a career foreign service officer, who left a senior position in the Department of External Affairs to become the first civilian to head the security intelligence function within the R.C.M.P. His appointment, effective January 1, 1970, was the first and most significant step taken by the government to implement the June 26th policy statement.

35. Testifying before us, Mr. Starnes stated that he was never shown Mr. Higgitt's letter to the senior staff of the Security Service and the heads of foreign agencies referred to above (Vol. C32, pp. 4016-4019). In hindsight, he noted that he was not surprised by the letter. By his own admission he was successful in effecting only a few minor changes in the management of the Service: a change in the name of the agency to the Security Service; civilian dress for Service employees; and separate identity cards (Vol. C33, pp. 4205-4215). He was not successful in his attempts to gain autonomy for the Service in three main areas — operations, personnel policy, and financial administration — a step he felt essential if the Prime Minister's statement was to be translated into a reality (Vol. C29, p. 3512).

36. Just before leaving the Service in March 1973, Mr. Starnes met with the Prime Minister to tell him about a study by a group of management consultants on the management and structure of the Security Service. (This study will be discussed later in this chapter.) He also told the Prime Minister, according to his testimony, that ". . . in fact we really hadn't done very much up to that point. . . by the time I left, there was no — we did not have control over our personnel resources or financial resources, in effect" (Vol. C33, p. 4223).

37. We have found no evidence that successive Solicitors General took initiatives to develop an implementation plan, or that they systematically monitored the R.C.M.P.'s progress in this area. For example, the Honourable Jean-Pierre Goyer, who served as Solicitor General from December 1970 to November 1972, testified that he left the implementation of the government's 1969 policy totally up to Mr. Starnes:

> Q. Did you deal with the question of structural changes, that is to say, recruiting more members or more non-members or non-constables into the Security Service so as to meet certain objectives which had been established? More civilians?
>
> A. No, no. That was up to Mr. Starnes. And it was not a subject with which I dealt in detail. My concerns were of a more general nature: recruitment policies; training policies and so on.
>
> (Vol. 122, p. 19062. Translation.)

38. The elements of the failure in implementation are clear: the policy statement itself, which contained no specific targets or dates and which was not followed up with a more detailed set of instructions; the absence of a clear implementation plan; the lack of any strong ministerial initiative on the part of the successive Solicitors General to ensure that implementation was proceeding; and, perhaps most important, concerted opposition to the policy statement from the senior management of the Force. As we shall see, these contributing factors remained more or less constant for the remainder of the decade.

39. In many discussions we have had with senior members of the Force about the Prime Minister's statement, they have used the statement's alleged imprecision as their primary defence for inaction. "What does '... increasingly autonomous in structure and civilian in nature' mean?" they have asked us. There are three rejoinders to this question: first, senior members of the Force were involved in lengthy discussions on the recommendations of the Royal Commission and the drafting of the Prime Minister's statement. Their own file material reveals this. Second, the R.C.M.P. has been unable to give us any instances in which their senior managers asked the government to clarify the policy statement. Third, while the statement lacks specifics, its general direction is clear, particularly in the last portion of the policy statement quoted earlier in this chapter. The Prime Minister was not ambiguous in announcing that there would be "new and more flexible policies in relation to recruiting, training, career planning and operations" so that an increasing number of university graduates from all parts of Canada could join the Service "in a civilian capacity" and "aspire to positions at the top of the organization". Relevant to this discussion about the alleged imprecision of the policy statement is the following question and answer sequence from the testimony of Mr. Dare, the current Director General of the Security Service:

> Q. Mr. Allmand, in his testimony... refers to a meeting when you were appointed, at which... the Prime Minister emphasized the need to continue with civilianization of the Security Service. Was that, in fact, suggested to you?
>
> A. That is correct, Mr. Chairman.
>
> Q. And do you consider that in the years before the Commission began, the policy of civilianization of the Security Service was carried out?
>
> A. No, Mr. Chairman.
>
> (Vol. C90A, pp. 12474-12475.)

Mr. Dare's unequivocal response indicates that he clearly understood the policy. The inaction within the R.C.M.P. in implementing it, therefore, boils down to one factor: the Force's senior management strongly opposed it.

The Bureau of Management Consulting's Report, 1973

40. As part of his attempt to effect change along the lines of the June 1969 policy statement, Mr. Starnes obtained agreement from Commissioner Higgitt in June 1972, to employ the Bureau of Management Consulting (B.M.C.), a component of the Department of Supply and Services, to undertake "a study of

organization and classification". Mr. Starnes, in his testimony before us, noted that he expected "... very far reaching proposals for change" (Vol. C33, pp. 4220-22).

41. A short summary of the report's major findings was presented to Mr. Starnes in March 1973. The actual report was not ready until Mr. Michael Dare, a former military officer, had become Director General. In July 1973, Mr. Dare wrote the senior administrative officer of the Force, advising him that the senior managers of the Security Service had reviewed the report and had accepted in principle its major findings and recommendations.

42. The most controversial recommendations concerned the relationship of the Service with the rest of the Force. The B.M.C. recommended that the Security Service be given managerial control over both its operations and the administration of its resources — human, physical, and financial. The B.M.C.'s concept of managerial autonomy was reflected in the following key paragraph from the report:

> In the concept of managerial autonomy we propose, the managerial link would be confined to the Commissioner, Director General level. There would be no influence from the administrative arm of the R.C.M.P. as to how the Service administers its resources in the execution of its mandate. Also, there would be no influence from R.C.M.P. Divisional Commanding Officers over both operational and administrative actions of Security Service field components. Control would be exercised by the central agency of the Security Service.[10]

43. The rationale behind this recommendation rested on two crucial premises:

(i) the mandate of the Security Service is intrinsically different from that of a police force and requires that "policies and programs must be controlled and monitored from within the Service."

(ii) the Director General of the Security Service lacks the delegated authority to manage this operation effectively.

44. The B.M.C. noted, however, that several factors support a concept of "managerial autonomy" *within the R.C.M.P.*: the excellent reputation of the Force; the need for the Service to maintain a secret budget; the utilization of services common to both activities; and the need for close liaison in regard to activities of interest to both the Security Service and the law enforcement side of the Force.

45. Other recommendations made in the B.M.C. report included adopting the principle of "centralization of policy and program control and decentralization of execution," revamping the planning process along "management by objectives" lines, flattening the organizational pyramid by reducing the number of supervisory levels, improving training programmes, and upgrading selection criteria for entry into the Service. The B.M.C. also noted that "morale could be considerably improved" and made several suggestions to accomplish this.

46. In contrast to their counterparts in the Security Service, senior managers from the rest of the Force were highly critical of the B.M.C. report. There was

---

[10] Bureau of Management Consulting's Introductory Report, 1973, p. 81.

virtually no support for its major recommendation concerning operational and administrative autonomy for the Security Service. Rather, both divisional commanding officers and senior administrative staff argued for the reverse situation for some of the following reasons, as noted in a record of the discussion:

— 95% of the Security Service want to remain with the Force;

— by becoming more autonomous, the Security Service could be easily "snipped away" from the Force by a "stroke of the pen" of some politician;

— commanding officers of field divisions complained of getting all the problems relating to the Security Service but none of the benefits (no consultation and information or none of the better personnel);

— there was a need for closer relationships between the criminal investigation side of the Force and the Security Service because of changing internal conditions within Canada (i.e. increased terrorism);

— there would be problems of "internal relativity and compatibility";

— costs would increase at a time of fiscal constraint;

— it would be difficult to establish responsibility if problems arose (who, for example, would be in charge of classification for the Force as a whole?).

47. In December 1974, Commissioner Nadon, his Deputy Commissioners, Mr. Dare, and several Assistant Commissioners, met to make decisions with respect to matters raised in the B.M.C. study. The minutes of that meeting indicate that the major recommendation concerning Security Service autonomy was rejected, that the Security Service was to be linked even more closely to the Force, and that few of the remaining recommendations relating to internal management and personnel of the Security Service were even recorded as having been discussed. At this point, the B.M.C. study would appear to have had an effect opposite to that intended by Mr. Starnes.

National division status

48. Following these discussions of the B.M.C. report by the Force's senior management, Commissioner Nadon received at least two requests to clarify the organizational changes he was contemplating for the Security Service. The first came from Mr. Gordon Robertson, the Clerk of the Privy Council, who directed his request to Mr. Roger Tassé, the Deputy Solicitor General. The second came from Prime Minister Trudeau who wrote to the Solicitor General, the Honourable Warren Allmand, in September 1975. The Prime Minister went immediately to the heart of the matter by noting that

> ...I have not had any report for several years on the progress that has been made to implement the government's decision that the Security Service of the R.C.M.P. should be made more autonomous in its structure and more civilian in its character. From information that has reached me, I have the impression that not much progress has, in fact, been made and if this is so, it disturbs me.

He ended his letter by asking Mr. Allmand to

> . . . let me have a report on this matter at your earliest convenience — both concerning the situation as of the present time and concerning the further measures that are in contemplation to achieve the result decided upon in 1969.

49. The Force's senior management began drafting replies to both requests, based on the results of the R.C.M.P.'s deliberations concerning the B.M.C. report. Basically, they were developing two proposals:

1. that no further steps be taken to separate the Security Service from the rest of the Force;
2. that there be greater integration of technical support and administrative functions with the rest of the Force.

50. A handwritten note by Commissioner Nadon to his senior administrative officer is indicative of the reaction he received from the Solicitor General's Department to these proposals:

> Solicitor General returned this to me today stating he believes we will have a hard time selling this to the P.M. He suggests we prepare a memorandum to P.M. along the lines of memo to Cabinet and that I should go and defend my position before P.M. personally. . .

51. Not surprisingly, the structural changes that were eventually approved in 1976, first by a committee of senior officials and then the Prime Minister, appeared — at least on the surface — to be quite different from the R.C.M.P. proposals. The Security Service became a "national Division" within the R.C.M.P. It was to have administrative responsibilities similar to those delegated to an R.C.M.P. geographical division (with a few exceptions, there is an R.C.M.P. division for each province) but it would be unlike other divisions in being national in scope. To create this "national division", Commissioner Nadon delegated additional authorities — both operational and administrative — to the Director General of the Security Service. Under the new operational authorities, the Security Service units in the field, which up to this point had reported to the head of their R.C.M.P. geographic division, began reporting to a Security Service officer based at Headquarters in Ottawa. This change formalized a situation which, in fact, was already largely in place. As Commissioner Simmonds noted in testimony before us:

> Right up until 1976 . . . the Security Service personnel in the field were underneath the divisional commanders for the purposes of administration and discipline, and so on, but their operations were to a very large extent centralized under the Director General at Headquarters, and thus there was a split. Operations reported one way, and yet for administration and discipline, it was another way, and it was not, in any view a very sound structure at that point.
>
> (Vol. 164, p. 25182.)

52. In commenting on the administrative changes, Commissioner Nadon explained in the documentation that went to the government in July 1976 that, "As a guide, the general administrative structures and authorities of the Security Service will be patterned along those of a Division of the Force with

the necessary adjustments to take into account the special needs and national character of the Security Service." How, in fact, the Force was going to interpret this broad statement became clear in an internal memorandum. Commissioner Nadon noted that any administrative policies that the Security Service would henceforth adopt would still have to be "in accordance with the legislation, regulations, policies, directives and guidelines applicable to other components of the Force". An article in the R.C.M.P.'s in-house newspaper, *Pony Express*, in December 1976, also tended to down-play the importance of these structural changes. A particularly telling question and answer sequence in the article was the following:

> Q. Where will the main impact of the reorganization occur?
>
> A. The reorganization will mainly affect the administrative side of Security Service, especially at the Headquarters level. Quite simply, Security Service Headquarters will be establishing administrative units to attend to these needs of members of the Service. The membership of Security Service can expect to see, in fact, very little change in what they have to do, administratively. The change will be that material formerly sent to each Divisional Headquarters will now be sent to Security Headquarters. In this way, there will be uniformity of policy and direction for all Security Service members. Also, Security Service members will be looked after by those who have knowledge of the needs of the Service.

53. Mr. Michael Pitfield, the new Clerk of the Privy Council, wrote to Commissioner Nadon in August 1976, a few weeks after the National Division changes had been approved by the committee of senior officials. Mr. Pitfield indicated that the Prime Minister had approved these changes and had noted that "... the arrangements which you have recommended provide the necessary authority for the Director General of the Security Service to work towards a greater emphasis on the civilian character of the Security Service".

54. The Security Service went to work immediately in August 1976, to implement National Division Status. Implementation was not completed until early 1978. We have no evidence, however, that these changes have resulted in any greater emphasis being placed "on the civilian character" of the Service. If anything, the current period can be characterized as one of increasing integration of the Security Service with the rest of the Force. The current Commissioner, Mr. Robert Simmonds, whose term as Commissioner began in September 1977 after the formation of this Commission, instituted a number of changes that are noteworthy in this regard. For example, the senior executive committee of the Force, consisting of the Commissioner, his three Deputy Commissioners and the Director General, must now approve all major operational policies of the Service. In addition, the Commissioner has established an operational audit unit specifically for the Security Service in order to give him another "window" into what is happening within the Service. Recommended changes resulting from these audits are discussed by a Force-wide Audit Committee. Finally, the Commissioner has made a number of senior appointments which have moved several officers with no prior Security Service experience into several of its most senior positions. As for the question of increasing the civilian character of the Security Service, Commissioner Sim-

monds testified before us that no progress is being made at the moment and that in his view what has already been done "may have gone too far..." (Vol. 165, p. 25377). According to Commissioner Simmonds, the Security Service, in future, should have ". . . a stronger peace officer connotation..." on the assumption that certain analytical functions now performed by the Service would be done elsewhere in the government.

The current situation

55. There is at least one other aspect of the current situation with regard to the management and structure of the Service which we find particularly noteworthy. On the basis of our experience in the hearings, the numerous informal meetings we have had with a great variety of Security Service members ranging from some of the most junior to the most senior, our own examination of Security Service files, and research done by our staff, we conclude that a desire for significant change exists at virtually all levels within the Security Service. Levels of dissatisfaction with current personnel policies within the Service are high, and often those holding these views see structural solutions (either more autonomy within the Force or complete separation) as the ultimate answer.

56. Our assessment of the current situation within the Security Service, summarized above, is not based on any research study which attempted to determine the opinions of a scientifically chosen sample of Security Service members. Having said this, we find it noteworthy that our assessment is compatible with two recent studies of the Security Service which produced statistical results. One such study was conducted by an R.C.M.P. audit team in March 1976 and the other was carried out by our researchers. In the R.C.M.P. study, questionnaires were distributed to members of the Security Service, and an impressive 80% were returned. The opinions and those favouring each were as follows:

	Option	Percentage of Respondents Favouring Each Option
1.	Remain an integral part of the Force and continue to function as it does now, retaining the current operational and administrative policies and practices.	21
2.	Remain an integral part of the Force and be governed by common Force administrative policies and practices.	6
3.	Remain an integral part of the Force, retain the current operational practices and be given more administrative autonomy than now exists.	47
4.	Become a completely separate entity outside the Force.	26
		100%

Thus, 79% of the respondents favoured changes from the status quo. While 6% favour closer integration of the Security Service into the R.C.M.P., 73% favour

change in the opposite direction. The most popular option, favoured by 47%, was greater autonomy within the R.C.M.P. 26% supported complete separation from the R.C.M.P.

57. The second study was an interview programme conducted by our own research staff in late 1978 and the early part of 1979. Participants in this study expressed nearly unanimously a desire for far-reaching changes. In all, our staff interviewed 38 members of the R.C.M.P., chosen on the advice of the R.C.M.P. unit responsible for liaising with the Commission so as to represent a cross-section of knowledgeable opinion. Each interview lasted between two and three hours. Of those interviewed, nine were civilian members and one was a special constable. The remaining interviewees were regular members of the Force, the large majority of them officers. Six participants were not members of the Security Service, but four of these had served in it for long periods. The average length of service within the R.C.M.P. was slightly over 21 years.

58. Those advocating significant change identified three possible directions:

1. *The Security Service should remain within the R.C.M.P. but have the necessary autonomy to fashion a management approach and personnel systems in keeping with its role.*

   This approach was favoured by slightly less than half of those interviewed.

2. *The Security Service should separate from the R.C.M.P.*

   This option was also favoured by slightly less than half of those interviewed, including a number of senior officers.

3. *The Security Service should remain within a significantly changed R.C.M.P.*

   This argument, put forward by three participants, was based on the premise that the management and personnel systems of the Force are as inappropriate to the rest of the Force as they are to the Security Service. Thus, they concluded, significant and dramatic change is needed in all areas within the R.C.M.P.

This interview programme was not based on any scientifically chosen sample. The results are nevertheless noteworthy because the desire for change was intensely felt and shared by a large number of long-serving and quite senior Security Service members.

59. The interview programme conducted by our researchers and our own interviews have disclosed that one group within the Security Service is particularly dissatisfied, even bitter, about the current situation. These are civilian members, especially those holding analytical jobs. One civilian went so far to describe the second-class status of civilians within the service as "administrative apartheid". Others feel just as strongly. Indeed, in the latter part of 1978, a number of civilian members prepared a brief for the committee chaired by Mr. Guy D'Avignon on the Review of Personnel Management and the Merit Principle in the Public Service. This brief was highly critical of R.C.M.P. practices towards its civilian members. The civilian members agreed not to

submit the brief on the undertaking of senior management of the Force to review and reply to the points raised in the brief. Nearly everyone we talked to in the Service acknowledged the need to find some solution to a problem which has been well known to the Force's senior management since 1955. This level of employee dissatisfaction, especially among civilian members, would be an unhealthy situation in any organization: but in a security service, which is especially vulnerable to "leaks" and — even more serious — penetration attempts by hostile foreign agencies, it is an intolerable and dangerous situation.

60. In the next two chapters we shall spell out the extensive changes we believe necessary to put the Security Service on a sound managerial and structural footing. We shall recommend these changes with two objectives in mind: first, to improve its overall effectiveness, that is, to help the Service provide more timely information of higher quality to government about the security threats facing Canada; and second, to reduce the risks of Security Service members committing illegalities and improprieties in the performance of their duties. To give the reader an overall sense of our basic directions in these matters, we shall summarize our views briefly in the final section of this chapter.

D. CONCLUSIONS

Understanding the past

61. All four attempts to change the Security Service reviewed in this chapter — the study conducted by the senior civilian member in 1955, the Report of the Royal Commission on Security in 1969, the Prime Minister's policy statement in the House of Commons in 1969, and the study of the Bureau of Management Consulting in 1973 — had a similar essential logic. Each recognized, to varying degrees, that there are significant differences between the functions of a security intelligence organization and the basic functions of a police force. These differences imply that a security intelligence organization requires a different set of managerial and personnel policies. In particular, a more experienced, better educated, broader type of individual is needed for security intelligence work. Consequently, to develop these different policies, the Security Service should either separate from the R.C.M.P. (the Royal Commission on Security) or have a significant degree of autonomy within the Force (the 1955 study, the Prime Minister's statement, the B.M.C. study.)

62. In addition to the similarity of their arguments, these attempts at change met with much the same fate. They had little or no impact, primarily because of stiff resistance from the senior management of the Force. Even the publicly announced policy statement given by the Prime Minister of Canada in 1969 was largely ignored by the Force over a ten-year period. The policy has not been substantially implemented, nor has the Force made a concerted effort to do so.

63. Why has each of these attempts at change met with so little success? Hearing the testimony of a large number of Force personnel, studying the

Force's management and personnel systems, seeing at first hand the recruit training programme in Regina and studying the curriculum, have all given us important insights in answering this question. To implement any of the major recommendations flowing from these studies would have been a wrenching experience for the Force. It would have meant a denial of what many in the R.C.M.P. hold to be the essence of the organization and the basis for the wide measure of support it has among the Canadian public. Let us enlarge on this proposition.

64. In the course of our inquiry, several people have compared the R.C.M.P. with a religious Order. One such person was the former Solicitor General, Mr. Goyer, who testified as follows:

> Q. Did Mr. Starnes tell you of any difficulties or reluctance he encountered in properly managing or administering the Security Service?
>
> A. I think Mr. Starnes was faced with the same problems which I explained I had, that is to say, when you are not a Mountie, you are strictly an outsider. The same thing is true of R.C.M.P. clerical staff, who are not Mounties, or of certain people who work in laboratories. They definitely feel that they have second-class status. It is unfortunate. What can you do to improve that situation? I don't know. It's a matter of establishing communication, confidence and, eventually, perhaps friendship. But I do not think that — I did not notice that Mr. Starnes was incapable of doing his work for that reason.
>
> Q. Did he tell you that he had difficulty establishing this communication of which you speak?
>
> A. Yes, but once again, in this sense: the same difficulty that I encountered at the beginning, which decreased but never really disappeared. You never become a member of the R.C.M.P. if you haven't been through Regina. You have to accept the mould. When you do, you are one of them. The same is more or less true in the Armed Forces, I think. And that is surely the way it is with the Jesuits, to draw the same comparison. (Vol. 122, pp. 19063-5. Translation.)

65. Certainly some of the primary characteristics of the R.C.M.P. are those normally associated with a religious Order. Force recruits are young, with few exceptions they enter the organization at only the lowest level, gradually work their way up a well-defined rank structure, and pursue a "generalist" career path. Thus, there is a significant degree of homogeneity in the membership of the organization. In addition, the recruit training of the Force is designed to be a mentally and physically rigorous experience — it is an "initiation rite", a process which moulds the individual in the image of the Force, an experience which develops an *esprit de corps*.

66. Loyalty to the organization is a norm of the Force. As far as possible the R.C.M.P. arranges for the training of its own members in needed disciplines, rather than recruiting professionals, so that their first loyalty is to the organization rather than to their profession. Moreover, joining the Force is meant to be, if not a lifelong commitment, at least one which spans the best part of a person's working life. The Force pension scheme, for example, discourages officers from leaving until they have served, usually, 35 years.

67. There is also an extensive and well-defined set of rules governing the conduct of members both on and off the job. For those who demonstrate disloyalty by deviating from the accepted norms of the organization the disciplinary procedures are harsh. Even now, the Commissioner has the power to arrest a member and to hold him in custody without trial for up to 30 days for certain Service offences, ranging from disobeying lawful orders to engaging in "any activity in which his involvement is not in the best interests of the Force". As Commissioner Simmonds noted in testimony before us: "I doubt if there is any organization that has set higher standards for itself and exacts more out of its members than this organization, if they go wrong" (Vol. 164, p. 25237).

68. Finally, the R.C.M.P. possesses a definite quality of insularity. It has difficulty accepting and working with "outsiders", as the testimony of Mr. Starnes, Mr. Bourne, and Mr. Goyer so amply demonstrates. Accompanying this insularity is a certain self-satisfaction which manifests itself in a variety of assumptions: that the organization is headed in the "right" direction; that the managerial ingredients that have worked so well in the past will continue to work in the future; and that staff members who are not regular members of the Force can, with few exceptions, perform only peripheral roles.

69. None of the characteristics we have outlined above is unique to the R.C.M.P. All organizations have at least some of these to varying degrees. But it is their combination and special emphasis within the Force which makes the R.C.M.P. distinct from the rest of the federal government departments and agencies, and the vast majority of non-governmental organizations. Given the importance of these characteristics, which have a long history within the R.C.M.P. and are essential elements in its traditions, it is not surprising that the four attempts at organizational change described in this chapter met with so little success. To have accepted these changes would have implied an influx of civilian members in middle and senior management positions, none of whom shared the Force's traditions and work experiences, and all of whom would be reducing opportunities for regular members. Such attempts at change are an anathema. To accept them would be akin to a religious Order allowing those who had not gone through the arduous process leading up to the taking of religious vows to influence an essential part of the Order's operations.

Our position on managerial and structural matters

70. In the following chapter on management, we shall be making recommendations which, in several respects, are similar to proposals that have been made in the past. We shall recommend that Canada's security intelligence agency be staffed with more experienced, better-educated personnel, with a wide variety of backgrounds in government, universities, police forces and the private sector, and that many of the other personnel policies of the current Security Service (those, for example, dealing with training and development, remuneration and career paths) be altered to "fit" this type of employee. But we shall also be departing from past studies in some important ways. We believe strongly that changes in internal management practices are a critical element in the package of reforms we shall be proposing to reduce the risks of future illegalities and

improprieties. Past studies paid little, if any, attention to this aspect of management, whereas for us it is a dominant theme which colours many of our recommendations in this area.

71. Following the chapter on management, we shall turn to questions of structure. Our major recommendation here will call for a security intelligence agency which is separate from the R.C.M.P. We shall weigh carefully the arguments for and against this structural change, but for us, a compelling argument in its favour is our belief that the managerial reforms which we think are necessary and achievable have little likelihood of being implemented, should the Security Service remain within the Force. Past history, and our understanding of what many within the R.C.M.P. cherish about their organization, strongly support this conclusion. We realize that there are costs involved in separating the Service from the rest of the Force — certainly in human terms and possibly in financial terms. (We shall examine this latter point in more detail in Part VI, Chapter 3.) But our judgment is that the benefits of a separate security intelligence agency outweigh these costs.

CHAPTER 2

MANAGEMENT AND PERSONNEL

INTRODUCTION

1. A security intelligence agency is a complex organization and managing it is no easy matter. The international and national dimensions of its work present challenges ranging from liaison with foreign agencies to communicating, sometimes under demands of secrecy, with a staff that is dispersed widely. To this broad spectrum of relations with provinces, states, and other agencies are added factors that, while more intangible, still pose challenges to management. These include: the need to control carefully the use of intrusive and secret investigation methods, with their potential for damage to Canadian liberal democratic values; the false romance with which spy novelists have glossed the public image of intelligence work, ignoring the methodical drudgery of day-to-day investigations; the lack of public recognition of success, coupled with the quick condemnation of error; the moral pressure on individuals of work that relies to some extent on deceit, manipulation and other practices inherent in the collection of intelligence about espionage and subversion; and finally, the constant fear of the penetration of the agency by a foreign agent, thereby spurring protective measures that may themselves offer complex challenges to management.

2. In sum, the management of a security intelligence agency is not a job for amateurs. But, paradoxically, there is a danger in describing it as a job solely for professionals. There are some connotations of the term 'professional' which we find attractive — for one, it suggests a high level of competence — but there are two aspects to 'professionalism' which are potentially dangerous to a security intelligence agency operating within a liberal democratic country. The first is that non-professionals (those not belonging to the agency) are seen to have little basis for making useful comments on important aspects of its work. Mr. Robin Bourne, a former assistant deputy minister in the Solicitor General's Department, in testimony before us, gave a good example of this tendency, when speaking of the Police and Security Planning and Analysis Branch of the Department.

> We did not interfere with operational policy. Now, the recruitment of sources — I am not saying we should have or shouldn't have. I am trying to explain why, even though you would interpret the terms of reference that way, we did not nor were we asked to involve ourselves in this kind of policy. If we had tried to in an unsolicited way, we would have been accused of interference in operations which are the business of professionals.
>
> (Vol. 142, p. 21768.)

In an area of government fraught with difficult political decisions and moral dilemmas, this tendency to exclude others because they are not professionals is both wrong and dangerous. Ministers and senior government officials must play an enlarged role in governing the affairs of the agency. Our second misgiving about professionalism arises from the tendency of professionals to give their first loyalty to their profession. We believe that security intelligence staff should give their primary loyalty not to their profession, nor to their employing agency, nor, especially, to the political party in power, but to Canada's liberal democratic principles which the agency has been established to protect. For these reasons, we do not recommend this kind of 'professionalism' as a distinctive quality of the staff of a security intelligence agency.

3. In this chapter, we concentrate almost exclusively on the 'human' side of managing. We say nothing about property management or computer management, and have only some brief comments to make on financial management. The basic principles put forward in this chapter should apply no matter where the security intelligence agency is placed within government. They are as relevant to a Security Service within the R.C.M.P. as they are to an agency separate from the Force.

4. We address first the question which is central to this Commission's work: why did people behave illegally and improperly, and what are the best approaches that an organization can adopt internally for preventing, as far as possible, the recurrence of such behaviour? Following discussion of this general question, we shall specify the requirements for the positions of Director General and other senior management and examine the appropriate personnel policies for the agency by considering such matters as recruitment, training and career paths. Recommendations in both of these initial sections aim at ensuring that the right people are doing the right jobs. In the latter sections, we shall turn our attention to how people relate to each other within the agency. We shall develop recommendations on leadership style, on approaches to organization, on how the agency should provide its legal and auditing services, and finally on internal security procedures.

A. THE IMPORTANCE OF INTERNAL MANAGEMENT

5. Our recommendations on the management of Canada's security intelligence agency will have two equally important objectives in mind: first, to enhance the agency's capacity to provide government with timely, high-quality information about security threats to Canada; and second, to ensure that the agency, in providing this information to government, acts in a manner which is both legal and proper. Because so many of our recommendations are coloured by concerns for reducing the risks of future wrongdoings, it is appropriate that we begin this chapter by explaining our basic approach to this matter.

6. What sort of internal policies can an organization such as a security intelligence agency adopt to minimize the risks of its members behaving illegally or improperly? Answers to this question depend upon assumptions about the causes of wrongdoings in organizational settings. One assumption is that people who do these acts are 'evil', and it leads usually to a 'battening

down the hatches' approach aimed at discouraging or uncovering deviant behaviour. Thus, the organization relies heavily on such approaches as auditing mechanisms, placing 'good' people in key positions, centralizing decision-making, and prescribing acceptable behaviour in great detail through the use of standardized routines and manuals.

7. There are costs involved in an over-reliance on such 'watchdog' or 'policing' type control mechanisms. They can produce a rigidity in the functioning of the organization and apathy in performance of individuals and, worse, their very existence may spur employees to try to counter or circumvent them. But our deeper concern is that the assumption on which they are founded — that wrongdoings are caused solely by, or even primarily by, 'evil' people — simply is not supported by the evidence before this Commission. We were not investigating acts of 'police corruption'. Most of those involved in wrongdoing would probably be considered exemplary citizens in their private lives — law-abiding, morally sensitive, public-minded, and so on. Why did these men act in the way they did?

8. There is no simple answer to this question, but our testimony does reveal that several factors were important. One of the most common rationales we heard was that the "ends justified the means". Consider the following testimony by a former Commissioner:

> Q. Am I correct to understand that the general rule of ethics is that the end does not justify the means?
>
> A. Yes, I think that is true, yes.
>
> Q. But when we come to security matters, there are situations where the end will justify the means?
>
> A. Yes, I think there are occasions when, as I have just explained, actions, all of which must always be reasonable — there are cases where actions are taken in the pursuance of Security Service, delicate investigations where actions that would not be justified under other circumstances can be justified.

And later:

> Q. So would you put a brake to your principle that the end does at times justify the means within the confinement of legality?
>
> A. No, I don't think I would be able to put that brake on it. It has got to be within the confinements of reasonableness.
>
> Q. And reasonableness can stand beyond legality?
>
> A. Yes, indeed, I think it can in certain circumstances.
>
> (Vol. 113, pp. 17457-17462.)

9. Those who put forward this rationale for acting illegally or improperly tended to emphasize the grave threats to national security which appeared to call for extraordinary means.

10. Another common justification used by many who appeared before us was that their actions were not based on a "guilty mind", that is, they argued that they had no criminal intent. The following, for example, are the comments of a

Security Service officer who authorized the publication of a false communiqué in the early 1970s.

> So, I don't believe that the publication of that communiqué would have been an offence under that section [of the Criminal Code dealing with forgery]. I don't know whether I would have been convicted of an offence under that section. I concede that because of the terminology, I might have been charged with such an offence; but I think that the intent — the intent to make a forgery, for example, which is important, was not there.
>
> (Vol. 65, p. 10705.)

11. Yet another common refrain which we heard in our hearings was that "I was only doing my duty". Thus, many witnesses saw themselves as not responsible for their actions. They were obeying the orders of their superiors, or, in some cases, conforming to policy approved at the Force's most senior levels. Here is a constable involved in an incident in which material was taken without the consent of its owner:

> Q. Did you ever consider whether the operation in which you were asked to participate was lawful?
>
> A. I considered it and felt that due to the reason explained to me by my superiors, that it was necessary, and it was needed at all costs.
>
> Q. What do you mean by that?
>
> A. Well, I felt in my mind it was necessary. . . . * had a source to establish in the milieu. What that source was involved in, or how sensitive his position was, I don't know. I presumed it must have been quite important for such an operation, and I was satisfied that if . . . *instructed . . . *and I to get a hold of such a thing, that it was necessary. I was not in a position to question it, sir.
>
> Q. Why were you not in a position to question it?
>
> A. Because I am a constable and . . . *is a Staff Sergeant. That's the reason.

12. Constables were not the only R.C.M.P. members to use the rationale of superior orders to justify their actions. Even a former Commissioner believed that he had faced the dilemma of superior orders:

> But, you know, I was a Commissioner and I was sitting in on some very high councils of this land when things were very difficult, and I was being told exactly what was necessary and what ought to be obtained if that were possible. Now, whether you take it as an instruction or a wish, I don't know, but as a Commissioner, I would not have remained in office very long if he [sic] had said, "There is no way". There has to be a way.
>
> (Vol. 87, p. 14358.)

13. Testimony before us on several occasions has pointed to the difficulty facing a member of the R.C.M.P. who might have questioned the orders of a superior. Former Commissioner Higgitt, for example, told us that a member was not forced to obey an unlawful order, but that refusal to follow such an order might result in an undesirable transfer. Commissioner Simmonds took a different approach to this question. He refused to accept the premise that

*Name deleted made pending disposition of possible legal action.

"... in this organization, a member would be afraid to question an unlawful order" (Vol. 165, p. 25521). But he went on to acknowledge the difficulties facing a junior member who might wish to question the orders of a superior, and suggested that the member's career would not be impeded *as long as he was right* (Vol. 165, p. 25525). (Our emphasis.)

14. Finally, we heard from a number of Security Service members who stated that questions of legality and propriety never entered their minds. Consider the following testimony on the matter of the letter sent to Mr. Allan Lawrence, M.P., concerning R.C.M.P. mail opening practices:

> Q. Well, had you had any discussion or concern with the senior officers about the legality or propriety of this operation?
>
> A. No.
>
> Q. Did it ever occur to you that it would be necessary or desirable for you to have such a discussion?
>
> A. I cannot say that it did, Mr. Thomson.
>
> Q. Why not?
>
> A. Well, I assumed — perhaps I was wrong to have done so — that the officers of the Force that would approve this sort of operation understood fully what it was about, and the ramifications of it and that it must be sanctioned by someone in authority at least. This is all retrospective analysis, because I cannot say that I really ever addressed my mind to the question at the time.
>
> (Vol. 159, p. 24309.)

Captured in the testimony is a troublesome aspect of modern organizations: long chains of command that separate the person who makes the decision from the one who executes. Who is to bear the consequences?

15. Another factor peculiar to a security intelligence organization which may help explain why so little attention is paid to these issues, is that the nature of the work, at times, dulls an individual's sensitivity to moral issues. Nowhere is this more graphic than in the development of informants or 'sources'. To be successful here, some contend, requires the condoning of ethically questionable activities. As one former member of an intelligence agency explains:

> ... the highest art in tradecraft is to develop a source that you "own lock, stock and barrel." According to the clandestine ethos, a "controlled" source provides the most reliable intelligence. "Controlled" means, of course, bought or otherwise obligated. Traditionally it has been the aim of the professional in the clandestine service to weave a psychological web around any potentially fruitful contact and to tighten that web whenever possible. Opportunities are limited, but for those in the clandestine service who successfully develop controlled sources, rewards in status and peer respect are high. The modus operandi required, however, is the very antithesis of ethical interpersonal relationships.[1]

[1] E. Drexel Godfrey, Jr., "Ethics and Intelligence", *Foreign Affairs*, Vol. 56, (April/July 1978), p. 630.

16. In pointing out some of the motivations which led to the allegations of wrongdoing investigated by us, we are neither condoning the behaviour nor suggesting that motives, no matter how noble, provide a legal defence for questionable behaviour. In Part IV, Chapter 1 of this Report, we have made our position quite clear on this point. What we are suggesting, however, is that motivations provide relevant clues for designing ways to prevent such acts in the future. The evidence before us suggests that the reasons for committing wrongdoings are complex and have at least as much to do with 'systems' failures — that is, failures in the systems of law, management, and governmental relationships affecting the Security Service — as they do with human failings. This conclusion leads to another: that to rely *solely* on control mechanisms which 'police' behaviour or require approval for action from some organization or individual outside the agency would lead to a system of controls which is less effective than it could be. We, therefore, stress a variety of approaches: some admittedly are of a watchdog type, but others aim at reducing or eliminating the characteristics within an organization that lead 'good' people to act improperly or illegally. These latter approaches are usually inexpensive, tend to operate more or less automatically in the day-to-day operations of the agency, and, if properly designed, will not produce organizational rigidities, or behaviour aimed at subverting their intent. One disadvantage of such approaches, however, is that they cannot usually be implemented in a short time period.

17. The recommendations we have developed on the mandate of Canada's security intelligence agency illustrate our belief in the need for a variety of approaches to encourage behaviour that is legal and proper. For example, we have recommended increased ministerial and judicial involvement in the process of approving the use of intrusive investigative techniques. But it is clear to us that such approval is no guarantee that those within the agency will use these investigative methods properly with due regard for the law. Therefore, it is equally important that there be no ambiguity as to how legality and propriety relate to other agency goals. For agency employees, it must be crystal clear that breaking the law will not be condoned or ignored in any circumstances, even if other agency goals are being met. Thus, clarifying the type of behaviour which is expected of agency employees is perhaps as important as changing the approval processes affecting the use of intrusive investigation methods. In this chapter, and those which follow, we shall continue to stress a variety of approaches, tailoring a particular approach to the likely motivations which might cause wrongdoings.

B. THE DIRECTOR GENERAL AND SENIOR MANAGEMENT

The Office of Director General

18. The very nature of a security intelligence agency — its operations shrouded in secrecy, its highly intrusive investigative techniques, and its interests in the political arena — explains why the relationship between the agency and the government has a high potential for abuse. On the one hand,

there is the danger that politicians or their senior officials will pressure the agency into providing information to be used for partisan purposes. For example, they might ask the agency to collect information about the private lives of certain political opponents in the hope that some of the information will be derogatory and therefore useful in discrediting these opponents. There is also the potential for the reverse kind of abuse: the security intelligence agency acts autonomously, with no effective direction and control of it by government. An extreme manifestation of this latter abuse occurs when the agency uses its covertly collected information to pressure politicians to achieve certain ends, such as increasing the agency's power within government, ensuring that the head of the agency is not fired, obtaining certain changes in policy, or preventing public disclosure of questionable operations. One of the major findings of the Church Committee in the United States was that both kinds of abuse had occurred:

> The Committee finds that information has been collected and disseminated in order to serve the purely political interests of an intelligence agency or the administration, and to influence social policy and political action.[2]

19. Choosing an appropriate person to be Director General of the security intelligence agency is one important means by which the likelihood of these abuses can be reduced. What are the desirable characteristics that a Director General should possess? First, he should be a person of "... high capacity and probity, and be accepted by the public and by others in government as having those qualities."[3] Second, in making this appointment, consideration should be given to individuals from outside the agency, although promotion to this position from within should not be barred. The following assessment in the study of the Central Intelligence Agency, conducted in the United States under the Chairmanship of then Vice-President Rockefeller, is relevant to Canada: "Experience in intelligence service is not necessarily a prerequisite for the position [of Director of the C.I.A.]; management and administrative skills are at least as important as the technical expertise which can always be found in an able deputy."[4] Third, the Director General should be knowledgeable about the various political and social movements in our society, should have a good grasp of international affairs, and should be experienced in the functioning of government. Moreover, he should value highly what the security intelligence agency is, in the end, securing — that is, the liberal democratic principles embedded in Canada's Constitution. And finally, it is important that the Director General's judgment on political matters be sound and unbiased.

20. In addition to choosing a Director General wisely, we believe it is important that certain aspects of his position should be structured to reduce the possibility of abuses. Our approach here is twofold. First, we shall make several

---

[2] United States Senate, *Final Report of the Select Committee to Study Governmental Operations*, Book II, 1976, p. 225.

[3] Australia, *Fourth Report of the Royal Commission on Security and Intelligence* (The Hope Report), Canberra, 1978, paragraph 385.

[4] United States, *Commission on C.I.A. Activities Within the United States*, June 1975, p. 93.

recommendations concerning how the Director General is appointed, his term of office, and how he can be dismissed. The point of these recommendations is to make it easier for the Director General to resist improper pressures from politicians and their advisors. Second, we shall recommend a series of checks and balances on the Director General's performance with the aim of ensuring that what his agency does is under the control and direction of government. In our discussion of the agency's mandate, we have already recommended one such device: the formation of a committee including several officials from outside the agency with responsibilities for controlling the use of highly intrusive investigative methods. In this section of the Report, we shall consider briefly the reporting relationship of the Director General as another check on the agency's operations.

21. In our opinion, the office of the Director General should be provided for in the legislation which creates the agency. That legislation should state how the Director General is to be appointed, to whom he is responsible and what his duties are. We shall deal with these three subjects in order.

22. Because of our strong belief that the government's activities in security matters should be removed from the realm of partisan politics, we feel that the Director General of the agency should be acceptable to all parties in the House of Commons. To accomplish this we consider that the statute should provide for the appointment of the Director General by the Governor in Council after consultation with the leaders of all opposition parties. We hope that an appointment made in this fashion will remove any taint of partisanship and will engender a degree of confidence which will facilitate the development of an effective relationship of the agency to Parliament. (We shall have more to say on this topic in Part VIII of this Report.)

23. We believe that the non-partisan appointment of the Director General will more likely help to avoid the kinds of abuses that we noted above by enhancing his office and thus providing him with the necessary strength to resist any improper pressures. We propose that his position be further strengthened by having his appointment extend for a term of years rather than "at the pleasure" of the Governor in Council. During that term he should be dismissable only for cause, and the grounds for dismissal should be set out in the Act. The Australian legislation has handled the matter as follows:

> 13. (1) The Governor-General may terminate the appointment of the Director-General by reason of physical or mental incapacity, misbehaviour or failure to comply with a provision of this Act.
>
> (2) If the Director-General
>
> (a) absents himself from duty, except with the leave of the Minister, for 14 consecutive days or for 28 days in any 12 months; or
>
> (b) becomes bankrupt, applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, compounds with his creditors or makes an assignment of his remuneration for their benefit,
>
> the Governor-General shall terminate his appointment.[5]

[5] Australian Security Intelligence Organization Act 1979, s.13.

We would recommend that dismissal for cause be defined to include physical or mental incapacity, insolvency or bankruptcy, misbehaviour or failure to comply with the provisions of the Act establishing the security intelligence agency.

24. The very strength of this proposal — that is, the difficulty the government would have in proving proper grounds for dismissal — also carries with it an inherent weakness. The government might find itself wishing to remove a Director General whom it regards as incompetent but without sufficient evidence to meet the statutory test. To reduce the likelihood of this, we propose that the Director General be appointed for a fixed term of five years. Such a provision has the additional advantage of providing a signal to both the media and the opposition parties, should the Director General resign or be dismissed before completing the full five-year term. In this situation, the government would likely be subjected to persistent questioning on what, if anything, has happened to explain his premature departure.

25. A final statutory condition on the appointment of the Director General is that the maximum period for which one person can serve in this position should be 10 years. Thus, the five-year term would be renewable only once. There are several advantages to this proposal. Ten years is long enough for any one person to head such an organization, since the Director General's job is a wearing one. A new Director General will bring new ideas and new approaches, and this fresh infusion will likely be healthy for the agency. A second advantage is that the Director General, after 10 years as head of a security intelligence agency, may know or be thought to possess much knowledge of a derogatory nature about politicians, senior officials and others in Canada. He might be tempted to use this knowledge as a lever to prolong his stay in office or for other questionable purposes.

26. We believe that the legislation, having thus established the office of the Director General, should then deal with his reporting relationships and the extent of his responsibility. Both the Australian and the New Zealand legislation have covered this question. The New Zealand Act states quite simply:

> (3) The Director of Security shall be responsible to the Minister for the efficient and proper working of the Security Intelligence Service.[6]

The Australian Act is somewhat more elaborate in its approach. It provides:

> 8. (2) In the performance of his functions under this Act, the Director-General is subject to the general directions of the Minister, but the Minister is not empowered to override the opinion of the Director-General —
>
> (a) on the question whether the collection of intelligence by the Organization concerning a particular individual would, or would not, be justified by reason of its relevance to security;
>
> (b) on the question whether a communication of intelligence concerning a particular individual would be for a purpose relevant to security; or
>
> (c) concerning the nature of advice that should be given by the Organization to a Minister, Department or authority of the Commonwealth.[7]

[6] New Zealand Security Intelligence Service Act 1969, s.5(3).

[7] Australian Security Intelligence Organization Act 1979, s.8(2).

27. We do not favour giving the Director General independent powers, as has been done in the Australian legislation. As mentioned earlier, we do not wish to give the Director General authority outside of a system of effective governmental control. Nor do we favour having the Director General responsible directly to the Minister. All the evidence before us leads inescapably to the conclusion that Ministers, although willing to exercise control over the R.C.M.P. Security Service, were unable to do so because they had no effective means of finding out what the Security Service was doing. In most cases members of the Security Service would no doubt have been willing to provide the Minister with whatever information he requested, although we have referred to cases earlier in this Report where members were less than forthcoming, and, in certain instances, intentionally misled the Minister — but the real difficulty is that the Minister has not known enough about the Security Service to know what questions to ask. He has been completely at the mercy of the Director General and the Commissioner of the R.C.M.P. With an agency whose operations are essentially secret we think this is not a healthy situation and we shall have more to say on this subject in Part VIII in dealing with ministerial direction. At this point we simply wish to deal with the lines of the reporting relationship.

28. The legislation should provide that the Director General is responsible directly to the Deputy Minister rather than to the Minister. The Deputy Minister would have the right to give direction to the Director General on all matters. Our purpose in recommending this structure is to counterbalance what would otherwise be the tremendous power in the hands of the Director General, given his control of a secret agency, the special method of approval of his appointment, and his tenure of office for a term of years.

29. The third area which should be covered in the legislation in relation to the Director General is the nature of his responsibilities. Once again it is instructive to turn to the Australian and New Zealand Acts. Each of them deals with the matter very simply. The Australian Act states:

> 8. (1) The Organization shall be under the control of the Director-General.[8]

The New Zealand Act states:

> 5. (1) There shall be a Director of Security who shall control the Security Intelligence Service.
>
> (3) The Director of Security shall be responsible to the Minister for the efficient and proper working of the Security Intelligence Service.[9]

We favour the very simple Australian statement, with the addition of the provision mentioned above that the Director General be responsible to the Deputy Minister and subject to the Deputy Minister's direction. Our recommendations on the responsibilities and the reporting relationships of the Director General will be found in Part VIII, Chapter 1.

---

[8] *Ibid.*, s.8(1).

[9] New Zealand Security Intelligence Service Act 1969, s.5.

30. Throughout our recommendations in this Report we have proposed that aspects of the security intelligence agency's functions be dealt with in legislation. We anticipate that the legislation would refer to the Director General as the person having certain duties and rights. For example, it would be the Director General who would contract on behalf of the Crown for the employment of staff. We think that this language is appropriate providing that there is the overriding clause that everything that he does is subject to the direction of the Deputy Minister. We should enter one *caveat* here. That is that in certain exceptional circumstances the Director General should have the right to go to the Minister 'over the head' of the Deputy Minister, or to the Prime Minister 'over the head' of both the Deputy Minister and the Minister. We do not consider that it is necessary to include this provision in the legislation. The circumstances in which we consider it to be appropriate will be set out in Part VIII.

A team approach to decision-making

31. We believe that no one person can possess all the qualities necessary to run such a complex organization as a security intelligence organization. Many factors make one-man rule obsolete, among them: the impact of new technology, both on the investigative side and in the area of information storage, processing, and communication; the increase in employee demands to influence decisions affecting them; the size of the agency's operations; the increasing need to 'work things out' with other government departments. Consequently, we believe it important to focus on the Director General and his team of senior managers — that is, the heads of the operational branches, the financial and personnel services, and the technical services of the agency.

32. We use the word 'team' quite deliberately. Because of the ever-present danger of an agent of a foreign power penetrating a security intelligence agency, the agency adheres to the 'need-to-know' principle. The effect of this principle is to restrict the flow of sensitive information within the agency. One problem, as the Rockefeller Commission pointed out, is that the application of the principle can easily lead to extremes:

> The compartmented nature of C.I.A. operations and the adherence to 'need-to-know' principles has restricted communication to lines of authority within each directorate. One directorate generally does not share information with another. The Director of Central Intelligence is, as a consequence, the only person in a position to be familiar with all activities. Therefore he is the focal point for formal internal control of the C.I.A.[10]

33. Having only one person in the agency familiar with all of its activities is undesirable for at least two reasons. First, there is a greater likelihood of the agency's embarking on activities of questionable legality and propriety. It is imperative, in our view, that the Director General receive advice from several sources on difficult decisions facing the agency — especially from those whose interests differ from the person initiating the proposed course of action.

---

[10] United States, *Commission on C.I.A. Activities Within the United States*, June 1975, p. 85.

Second, the quality of decisions is likely to be higher if taken with the assistance of a group of senior managers.

34. We have seen little evidence of an effective senior management team functioning within the Security Service. The Director General and his senior managers do not have regularly scheduled meetings, nor is there any indication that they as a group are the focal point for significant policy or operational decisions. In October 1979, the Commissioner of the R.C.M.P. approved the terms of reference for the Operational Priorities Review Committee (O.P.R.C.), a group whose existence was acknowledged two years earlier in November 1977. The O.P.R.C. is composed primarily of managers from operational branches along with a Department of Justice lawyer and an officer from the criminal investigation side of the Force. While the formation of this group is potentially a positive development, it cannot adequately replace a senior management team whose members should encompass all of the major areas of the Service. There are many policy questions, which, because of the operational orientation of the O.P.R.C.'s mandate, will not likely be tackled by this group. As well, significant operational decisions should not be left primarily in the hands of operational managers, nor similarly should administrative issues be dealt with solely by administrative staff. A senior management group drawn from various sectors ensures that countervailing pressures are brought to bear on major decisions.

35. In recommending the formation of a senior management team, we are not advocating the abolition of the need-to-know principle, at least as it applies to the senior managers of the agency. Rather, we are suggesting that common sense should prevail. The senior managers should direct their collective attention to only the most sensitive operations, and even here they can make informed decisions without knowing certain highly confidential information — for example, the actual names of informers.

36. One of the important tasks of the Director General is to ensure that he and his senior managers function as an effective team and that the make-up of this team reflects the strengths and experience necessary for making important agency decisions. Thus, several senior managers should have wide experience in other government departments and agencies, particularly those whose functions are relevant to security intelligence work, in order to encourage the infusion of new ideas and fresh approaches. Several should have an extensive investigative background, especially in counter-intelligence work. It would be desirable if at least one of the team members were a lawyer. (This person would not act as the legal adviser to the agency, a role which we shall explain later in this chapter.) All of the team members should place a high priority on effectiveness, on conducting agency operations legally and with propriety, and on upholding liberal democratic principles. Finally, at least one of the senior management team should have extensive knowledge of modern management methods and theories.

WE RECOMMEND THAT

(a) the Director General should be a person of integrity and competence; he should have proven managerial skills but need not have prior

working experience in security intelligence matters; he should be knowledgeable about political and social movements, international affairs and the functioning of government; he should have a high regard for liberal democratic principles; and he should have sound political judgment, not affected by partisan concerns;

(b) the appointment of the Director General of the Security Intelligence Agency be made by the Governor in Council;

(c) the Prime Minister consult the leaders of the opposition parties prior to the appointment of the Director General.

(69)

WE RECOMMEND THAT the following conditions of employment for the Director General should be included in the statute establishing the security intelligence agency:

(a) the Director General can be dismissed only for 'cause';

(b) 'cause' includes mental or physical incapacity; misbehaviour; insolvency or bankruptcy; or failure to comply with the provisions of the Act establishing the agency;

(c) the Director General should be appointed for a five-year term;

(d) no Director General may serve for more than 10 years.

(70)

WE RECOMMEND THAT the Director General and his senior managers act as a team in dealing with important policy and operational matters affecting the security intelligence agency.

(71)

WE RECOMMEND THAT Canada's security intelligence agency encourage the infusion of new ideas and fresh approaches by ensuring that a reasonable number of its senior managers, prior to joining the agency in a middle or senior management capacity, have worked in other organizations.

(72)

WE RECOMMEND THAT the senior management team of Canada's security intelligence organization have a wide diversity of backgrounds, reflecting experience in both governmental and non-governmental institutions, in the law, in investigatory work, and in management. All of the agency's senior managers should place a high priority on effectiveness, on conducting the agency's operations legally and with propriety and on upholding liberal democratic principles.

(73)

C. PERSONNEL POLICIES

37. In this section, we use the term 'personnel policies' to encompass the following matters:

— the kind of personnel required in a security intelligence organization;

— methods of recruiting personnel;

— policies relating to secondments;

— career paths within the organization;

— training and development procedures;

— whether or not agency employees should be members of the Public Service of Canada;

— whether or not agency employees should be allowed to form a union;

— counselling, discipline and grievance procedures;

— procedures for dismissing employees.

These matters do not exhaust the possible list of personnel policies relating to a security intelligence agency, but, in our view, they are the most important. We deal with each in the order given above.

Required personnel for a security intelligence organization

38. The R.C.M.P. is predominantly a career service. By this we mean that new members, with few exceptions, enter the organization at the lowest rank, and then proceed to work their way up the various levels of the organization, through a combination of seniority and merit. Thus, all the senior managers of the Force, including those within the Security Service with the exception of the Director General, have 'come up through the ranks'. Within a career service, there is little or no recruitment of middle and senior managers from outside the agency.

39. This system, as applied to the Security Service, has some obvious strengths. It ensures, for example, that the Service has a very experienced group of senior managers — nearly all have spent at least 25 years in the Force, some even longer. Until recently, those who have joined the Security Service have tended to remain in it for most of their career. The fact that all the senior managers and a large majority of middle managers of the Service have police backgrounds enhances cooperation with other police forces and ensures that investigative experience is brought to bear in decision-making. In addition, the common set of work experiences and traditions creates an *esprit de corps* amongst regular members of the Service, and this is an important asset.

40. Nonetheless, a career service concept as applied by the R.C.M.P. to the security intelligence function does not appear to us to provide the Security Service with the type of personnel required to perform its responsibilities effectively. Some commonly shared weaknesses among Security Service personnel are the following: a lack of knowledge of international affairs, a poor capacity for legal and policy analysis, a lack of sufficient experience in working with Ministers and other government departments and a serious deficiency in management skills and expertise. In addition to these weaknesses, R.C.M.P. career service employees tend to allow their powerful, inbred loyalty to the organization to overshadow other important responsibilities. Each of these points requires further elaboration.

41. Of the commonly shared weaknesses among members of the Security Service, the lack of extensive knowledge of international affairs is one of the most serious. In our research on the Service's relationships with foreign agencies we have found considerable evidence of this weakness. For example, on a number of occasions the Service has not demonstrated sufficient concern

about the foreign policy implications of its relationships abroad, nor has it, until very recently, shared sufficient information with External Affairs officials about these relationships. Lack of knowledge of international affairs or sensitivity to its implications also manifests itself in the analysis by the Service of activities of foreigners in this country. In paper after paper that we have examined, the Security Service analysts have not paid sufficient attention to the foreign policy context of what they are reporting on, nor have they demonstrated a sufficiently well-developed conception of what constitutes proper and improper diplomatic behaviour. The long history of poor relations with the Department of External Affairs is one legacy of this weakness in the international area. An uneasy relationship between a security intelligence agency and External Affairs may be an inevitable consequence of the difference in functions of the two organizations; nonetheless, the relationship has been far worse than it needs to be. The Security Service senior managers must bear their share of the responsibility for this.

42. Another shared weakness among members of the Security Service over the past decade has been an inadequate capacity for legal and policy analysis. The Royal Commission on Security pointed out this basic weakness in 1968, and we have seen little evidence of any marked improvement in this area. In the numerous meetings we have had with Security Service personnel on issues with clear policy and legal implications, we have been struck by the general absence of truly creative thinking. Policy papers by the R.C.M.P. which we have examined have been, with few exceptions, poorly structured and one-sided. They do not present the issues in a coherent and compelling fashion, and they demonstrate a lack of sensitivity to points of view other than those current within the Force. The papers have not analyzed clearly and cogently the powers required by an intelligence agency. In addition, there is little evidence of an attempt to balance the requirements of the agency with the important values of a liberal democratic society.

43. An insufficiently high level of managerial skills is yet another common weakness we have observed in the senior management and, indeed, in others within the Service. Extreme dissatisfaction among Security Service personnel, especially civilian members, is one indicator of this weakness. Another is the lack of any systematic, continuing programme within the Service to evaluate the 'products' in terms of the costs of producing them. We have seen, for example, no careful evaluation of any operations on a cost/benefit basis. Finally, as in our other discussions with R.C.M.P. members on policy matters, we were not impressed with the level of analysis brought to bear by senior people within the Service and the Force as a whole in meetings we held on management issues. There was little creative thinking on their part about the range of options a security intelligence agency might employ to ensure behaviour that is proper and legal. Moreover, we heard few worthwhile suggestions as to ways to deal with several serious problems facing the Security Service in the personnel area (for example, the lack of continuity of staff in the operational branches).

44. So far, we have been stating the case that members of the Service have, over the past decade, shared a number of common weaknesses which have

reduced the effectiveness of the Service. There is an important corollary to this argument. When a career service like the R.C.M.P. finally perceives a weakness in its staff make-up, it takes a long time to correct, especially in the senior management ranks, simply because the most expeditious solution — hiring someone from outside the agency — cannot be used. Two illustrations will help make this point more cogently. The first is the small number of francophones in senior positions within the Service. As of January 1980 there were only three officers above the rank of inspector whose first language was French. Given that one of the most complex and potentially volatile problems facing the Service may well originate in the Province of Quebec, this statistic indicates a serious myopia. Yet within a career service it is difficult to correct easily. The only option is to move francophones from the criminal investigations side of the Force, but the problem with that is that these individuals will not likely have any experience in security intelligence work.

45. A second illustration concerns women. The Force began recruiting women for the first time in the mid 1970s. Under current personnel practices, this means that no woman can reach a senior management position within the Service until well into the 1990s.

46. In addition to the inherent costs of a career service concept already noted above, there is at least one other, namely the tendency of career service employees to demonstrate an excessive loyalty to the organization. Indeed, recruiting and training practices are geared to foster this. The senior officer at the R.C.M.P. recruit training centre at Regina told us that underlying the emphasis at the training academy on physical conditioning and mental awareness was the objective of having the recruit "identify with the Force....":

> The whole of those first six months for a new member is an admixture of physical exertion, mental exercise, emotional testing and conditioning. Long days that start at six in the morning and end at ten at night. It is totally exhausting particularly during the first several weeks but it serves to test the strength of his commitment. It can be seen as his initiation into the Force. Its successful completion gives the candidate a sense of having accomplished what others before him have done, hence it is his license to belong. That is perhaps the strongest identity factor we have. Most members will tell you they were proud of having done it but would not want to do it again.

47. While building this type of organizational loyalty has its advantages, a significant cost, at least in the Security Service, is that the commitment to liberal democratic principles, including the rule of law, may become secondary. As we have made abundantly clear in other chapters of this Report, the disregard of these principles by Security Service members has been the most worrisome aspect of the Service's performance over the last 10 years. We are not suggesting that the career service concept was the sole or even primary cause of the illegal and improper acts which we have investigated. Rather, it simply did not provide any kind of check on these activities. Thus, there should be no equivocation in the future on this point. The primary loyalty of the senior managers (and indeed other staff) of Canada's security intelligence agency should be to the liberal democratic principles embedded in our constitutional

system rather than to the organization itself or to the security intelligence profession.

48. Given the costs which we believe are associated with having senior and middle managers with little or no experience in other organizations, we do not find it surprising that few organizations outside the police community adhere to such a system. Even some police forces have changed their thinking. In the United Kingdom, for example, no one can be appointed chief constable of a district police force without having served in another force.

49. We have recommended that a reasonable number of the agency's senior management, prior to joining the agency in a middle or senior management capacity, should have worked in other organizations. In making this recommendation, we wish to make it clear that it would still be possible, and indeed desirable, that some people who join in a relatively junior capacity have a full career within the agency. Once the implementation phase for creating the new agency is completed, we would envisage that the large majority of those entering the agency with experience in other organizations would do so at middle management levels and only occasionally at senior levels. This practice would ensure that those within the agency are not discouraged from seeking full careers within it, and would still make it possible for the agency to have a senior management team with a diversity of backgrounds. What are desirable work experiences for agency employees to have? Many should have experience in other government departments and agencies such as External Affairs, Industry, Trade and Commerce, Employment and Immigration, Solicitor General, Privy Council Office, and the Treasury Board. Police experience, while it should be a prerequisite for only a small number of specialized positions, should continue to be valued within the agency. Still others should have experience in universities, business, or labour unions.

50. Having a university degree should not be a requirement for joining the agency. University training is no guarantee of competence in the analytical, investigative or other types of skills required in security intelligence work. Nor is attending university the only means of obtaining these skills. Nonetheless, the agency should actively seek university graduates on the assumption that many who have attended university will have both the inclination and ability required for security intelligence work. At the very least, it should not restrict recruitment primarily to a pool of police candidates, 90 per cent of whom did not have university degrees upon entering the Force. Tables 1 and 2 below give some indication of those members of the Security Service who now have degrees:

Table 1

Percentage With Degrees — 1979

Regular Members	21.4%
Civilian Members	26.3%
Special Constables	1.6%

Table 2

Percentage of Regular Members With Degrees by Rank — 1979

Officers	42.8%
Staff Sergeants	13.2%
Sergeants	17.8%
Corporals	18.7%
Constables	26.3%

In our view these percentages should be substantially higher.

51. In addition to hiring more people with university degrees, a security intelligence agency requires people with training in a wide variety of disciplines, including languages, social sciences, physical sciences, liberal arts, administration, and law. Indeed, no particular degree should be declared irrelevant to the agency's work: an essential requirement is rather a capacity to obtain and weigh evidence, a capacity which may be developed in any of the intellectual disciplines. The Table below indicates to us that there has been far too much emphasis on degrees in political science and not enough on other disciplines — in particular law, administration, economics, and languages.

Table 3

Disciplines in Which Regular Members Obtained Degrees (As of 1979)

	% of total degrees
B.A.s	
Political Science	50
Sociology	7
History	8
Psychology	6
Economics & Commerce	4
Other	12
B.Sc.s	
Geology	1
Engineering	1
Chemistry	1
Physical Education	2
Public Administration	2
Zoology & Biology	2
Post Graduate Degrees	4
Total	100%

52. The question of language skills requires further exploration. Below is a breakdown of members of the Security Service who have a second language capability in other than the two official languages.

Table 4

Language Capability by Function — 1979

	Percentage with Language Capability in other than the Two Official Languages
Translators/monitors	48.4%
Investigative Roles	10.2%
Analytical Roles	17.42%

The statistics may overstate the situation. The language capability is self-assessed, and thus the statistics are likely to be on the high side. Even more important, those with a language capability, especially in the analytical and investigative roles, are not likely to use this capability for long because of the rate of mobility within the Service. (We shall provide more details concerning this problem in the next section of this chapter).

53. While attempting to attract people with a variety of work backgrounds and educational experiences, the agency should be looking for some characteristics common to all of its employees: discretion; emotional stability; maturity; tolerance; the capacity to work in an organization about which little is said publicly; no exploitable character weaknesses; a keen sense of, and support for, what the security intelligence agency is ultimately securing (i.e. democratic processes, structures and values); and political acumen. Perhaps patience should be added to this list as well, given the long-term nature of security intelligence targets. Security intelligence work can be frustrating for action-oriented individuals, who become bored with the slow pace at which investigations sometimes move.

Recruitment procedures

54. To recruit the experienced well-educated type of staff with the variety of backgrounds outlined above, the security intelligence agency will need to modify substantially its present recruiting procedures. In particular, it will need to make three important changes: first, the agency must widen the pool from which it recruits its staff; second, it should have only one category of employee, apart from support staff; and third, the agency should employ a wide range of recruiting techniques to determine those best suited for security intelligence work. Before developing each of these themes further, we shall summarize briefly current Security Service recruiting procedures.

55. Four distinct categories of employees work for the R.C.M.P. Security Service — regular members, civilian members, special constables and public servants. In addition, within the regular member category there are two distinct sub-categories, non-commissioned officers (N.C.O.s) and officers. For reasons never satisfactorily explained to us, N.C.O.s receive full pension benefits after 25 years service whereas officers must serve longer — usually 35 years — to receive full pension benefits. N.C.O.s are eligible for overtime pay while officers are not, and have separate eating and social facilities.

56. Briefly, the current recruitment policies for each of these four categories are as follows. The Security Service acquires all of its regular members from within the ranks of R.C.M.P. regular members serving with the criminal investigation side of the Force. Interest in the Security Service is identified through a computerized system which is updated regularly. When vacancies occur, the Security Service staffing branch reviews the list of all regular members who have signified such an interest and interviews those who, among other things, have "a balanced political perspective", above-average performance rating, "a demonstrated interest and capability in pursuing post-secondary education", and no restrictions on mobility. Candidates who complete the interview successfully must then have a security clearance interview prior to joining the Service. The Security Service rarely recruits corporals, sergeants or officers. Almost all the regular members coming into the Service have three to five years experience and are at the constable level, the lowest R.C.M.P. rank. The one exception to this general rule is in the centralized functions — administration, finance and personnel. Thus, to a large extent, the Security Service is a career service within a career service.

57. We shall now describe the procedures by which regular members are recruited by the R.C.M.P. itself. The procedure is essentially as follows:

- initial contact with an applicant is usually made by members stationed at detachments across the country;
- the detachment determines if the applicant meets minimum requirements for engagement;
- if so, the applicant is required to write a 3-hour general knowledge test;
- if successful up to this point, the applicant is interviewed by Division staffing and personnel branch (the interview includes a second test — this time a psychometric test);
- if the interviewer recommends engagement, then a thorough background investigation is conducted;
- if no information of a serious derogatory nature turns up, the applicant's name is added to the waiting list.

58. There are several salient points about this recruiting process. First, it is geared for entry into the R.C.M.P. at the constable level. Over the past decade, only a very small percentage of members have entered the R.C.M.P. at other than the lowest rank. (An example of an exception was the hiring of a band leader who was immediately promoted to inspector.) Second, only a small percentage of those recruited through this process are university graduates. In May 1979, of 770 people who had successfully met the minimum requirements and who were on the waiting list, only 77 (or 10%) had university degrees. Another 100 had some post-secondary training. Third, R.C.M.P. recruits tend to be young. The minimum age for joining the Force is 19. The average age of those on the waiting list in May 1979 was just over 22 years. Fourth, candidates must meet a certain combination of physical and educational standards to qualify. For example, a male under 5 feet 6 inches in height, with a university degree, but no prior police experience, could not become a regular member of the R.C.M.P. And finally, the recruiting process is based on

meeting minimum standards, not on achieving the highest scores in the recruiting process. Thus, an applicant who achieved the minimum standards as of January 1, 1980, would be chosen for training before a candidate in the same geographic area who scored higher but who went on the waiting list as of January 10, 1980. As one staffing officer explained to a member of our staff, the Force does not want "all race horses".

59. The recruitment procedures for civilian members and special constables are more easily explained. The selection criteria are quite general, reflecting the diversity of employees covered by these two categories (they range from clerical employees to highly skilled specialists in the computer and research/analytical fields). The only common qualifications are that all candidates must be Canadian citizens and at least 19 years of age. Personal acquaintance with a serving member appears to be the primary means of identifying prospective employees in these categories. Advertising and recruiting visits to universities are secondary methods. For specialist or technical jobs, candidates are interviewed by a board comprised of Force members expert in the field. Security Service staffing personnel also interview all candidates and administer two selection tests used by the R.C.M.P. for regular member recruiting. Finally, recommended candidates are subject to a security clearance.

60. Recruitment procedures for public servants, who are employed by the Security Service primarily in clerical jobs, are the same as those for the Public Service as a whole. These procedures are administered by the Public Service Commission and are subject to the Public Service Employment Act.

61. The above description of current Security Service recruiting procedures leads to several conclusions. The most obvious is that the recruiting base from which the Security Service draws its employees is far too narrow. In our view, it is ludicrous for a security intelligence agency to limit its primary source of recruits to those who have joined a national police force, generally at a young age with little or no experience in other organizations and with limited educational achievements. Over the past 25 years, the R.C.M.P. has recognized the inherent weakness of these recruiting practices in a variety of ways. One of the most important was creating a civilian member category for specialized jobs in technical and analytical areas. This solution, as we noted in the last chapter, has created additional managerial and morale problems which have plagued the Force for two decades. Similar problems exist because of the creation of a special constable category. There are even serious problems associated with the Force's having two types of regular members, officers and N.C.O.s. This is illustrated by the following testimony of a senior officer in the Security Service:

> Q. So, to put it bluntly and admittedly rather simply: you get a Staff Sergeant (an N.C.O.) who is looking at a possible promotion (to the officer ranks). It is going to cost him money in his pocket. You let him do another ten years before he can go on pension and subject him, at a time when his family may require his attention, to the probability of many moves, and at the same time, he knows full well that he can go out into the civilian sector and get a very attractive monetary offer.
>
> R. Yes.

Q. And I suggest to you that the result of that is, you said: you lose a lot of good people when they are becoming particularly effective?

R. Yes, that's generally in the time of their career when they are most productive because of their expertise.

(Vol. C20, pp. 2599-2600.)

In our opinion this problem requires very careful consideration by government, not only from the point of view of the Security Service, but with regard to the whole Force. We will look at this further in Part X, Chapter 1.

62. Apart from support staff, the security intelligence agency should have only one category of employee, which we shall refer to as intelligence officers. In keeping with the type of individual we hope the security intelligence would attract, we also recommend that intelligence officers not be given ranks used by the military or police, such as sergeant and inspector.

63. One purported advantage of current recruitment procedures, cited by several Security Service members in discussions with us, is that they reduce the risk of penetration — that is, of a foreign intelligence agency having a spy within the Security Service. Indeed, this argument, as the reader may recall from the last chapter, was put forward by the Force as a rebuttal to the recommendation of the Royal Commission on Security that there be a Security Service separate from the R.C.M.P. In essence, those making this case cite the uncertainty which a spy joining the R.C.M.P. would face as to whether he would even be successful in gaining entrance to the Security Service. He first must serve up to three years in a general policing role and, at that point, might find that instead of being admitted into the Security Service he is reassigned to other general policing duties. Thus, instead of penetrating the Security Service, he might well end up on traffic duty in a remote provincial town.

64. In our view, it is difficult for anyone, even those within the Security Service, to make this argument (or indeed, the counter-argument) with any degree of certainty. The reason is obvious. We are not likely to know the extent to which foreign intelligence agencies have penetrated the Security Service until well after the event, and even then the histories of spying activities are usually shrouded in doubt. The best one can do with this argument, therefore, is to make a judgment supported by what evidence there is. Our judgment is that current recruiting practices for the Security Service do not significantly reduce the risk of penetration. Regular members of the Security Service can be recruited as spies by foreign agencies. In an age when there are few illusions about East Bloc Communism, this method of recruiting spies, based usually on blackmail or bribes, would appear to us to be potentially more fruitful than first recruiting an agent on ideological grounds, and then having the agent attempt to join the R.C.M.P. and be transferred to the Security Service.

65. The experience of the Security Service over the past 30 years would appear to support this point. The Security Service has advised us that during this period the Service was penetrated. In a case which we examined closely, it was a regular member who, after joining the Security Service, was recruited to spy for a foreign intelligence agency.

66. A second point is that the penetration argument applies to less than half of Security Service employees, for civilians, special constables and public servants enter the Service by other routes.

67. Finally, it is significant to us that many experienced Security Service personnel do not take this argument seriously. As one senior staffing officer told us, a foreign agent with a university degree and a language capability who joins the R.C.M.P. is very likely to be accepted into the Security Service within three to five years. Another very senior officer summed up his views this way in a speech to his colleagues during a commanders' conference in 1974:

> We have a large number of employees of various categories. Some of those employees are not well paid; some have left themselves open to compromise; some may have sold out for purely venal reasons; some may have been recruited prior to employment with us. I do not differentiate between the various categories of employees. I disagree with the very dangerous assumption held by some to the effect that Regular Members recruited from the Law Enforcement side are more or less immune to coercion.

68. The thrust of our recommendations concerning recruitment thus far has been to enlarge the pool of people from which to draw suitable candidates for security intelligence work. The question now centres on how agency recruiters should attract candidates from this enlarged pool. We believe that an 'old boy network' should not be the primary means of recruitment: events in other countries have shown that such a network is no protection against spies — indeed, it can lull the agency into complacency about its employee-screening procedures. Moreover, this method of recruitment may not ensure the fresh infusion of new ideas and perspectives which we believe to be important for an organization prone to insularity. This is not to argue that the agency should discourage its employees and ex-employees from giving advice on recruitment matters. Rather, we are proposing that such advice be supplementary to a more open process of recruitment, much like that employed by other organizations looking for the same type of mature, experienced, well-educated individual. Thus, agency recruiters should visit university campuses, should encourage applicants from police organizations, provincial governments, and of course federal government departments, and, from time to time, should advertise in the newspapers. (Both the Australian and New Zealand security intelligence agencies have recently advertised for candidates through newspapers.)

69. To accompany this more open approach to recruitment there will need to be more rigorous security screening procedures (this topic will be expanded in a later section of this chapter) and a well-developed process for choosing those candidates best suited for security intelligence work. Currently, in the Security Service, staffing officers rely almost exclusively on a two- to three-hour interview to judge candidates. We believe that other means should be employed as well. For example, psychological testing should be used to help identify those who are clearly not suited for this type of work, although it will be of little help in determining who would be successful intelligence officers. Techniques like discussion groups can be used to assess a candidate's attitudes towards dissent, deviant behaviour and minority groups. In addition, the agency should develop means of testing the writing and analytical capabilities of its potential new

members. As another example, agency personnel should discuss with prospective employees, perhaps along with their spouses, the types of constraints which working in a security intelligence agency places on a person's life, such as the problem of not being able to say much to friends or spouses about the nature of the work.

70. We make one final comment on the process for recruiting agency personnel. In our view, one of the deficiencies of the Security Service's current approach to recruitment is the lack of involvement of senior operational officers. Experienced intelligence officers from the main areas of activity should be involved with staffing 'specialists' in both the process of designing recruiting policies and the process of deciding who should become members.

Secondments

71. The use of secondments (temporary interchanges of personnel with other institutions) is another way in which the security intelligence agency can develop a staff with diversified work experiences. At the same time, it can benefit from those who have spent a significant portion of their working lives in other institutions. Mr. Starnes, the former Director General of the Security Service, testified before us as to the difficulty of achieving an interchange of personnel between the Security Service and the rest of government:

> . . . I thought that there should be a lot more interchange between members of the Security Service and individuals in other government departments. And, in particular, having members of the Security Service assigned to other government departments, to give them some feeling for the scope of the government's work as a whole, and some knowledge how other government departments faced their various problems. In this area, I would, perhaps, get an agreement in principle, but then when it came to actually assigning someone to another government department, that agreement wouldn't be forthcoming in a concrete way; and, so, I would say that that would be an example of a step forward and then a couple of steps backward. Eventually, after a good deal of pushing and shoving, we did, in fact, get a number of people assigned to other government departments, but it was not a readily accepted thesis.
>
> (Vol. C33, p. 4205.)

72. The number of secondments actually achieved during the last 10 years appears to support Mr. Starnes' testimony.

Table 5

Secondments to and from the
R.C.M.P. Security Service 1971-1980

Secondment to the Security Service from	
— External Affairs	3
— Department of Justice	1
— Other (outside the Government of Canada)	5
TOTAL	9

Secondments from the Security Service to	
— Solicitor General's Dept.	7
— External Affairs	3
— Privy Council Office	2
— Other (outside the Government of Canada)	5
TOTAL	17

Both the number of secondments and the the number of institutions with which secondments are arranged should increase. In addition to exchanges with other agencies, federal government departments, and the R.C.M.P., the security intelligence agency would benefit from an interchange of personnel with such organizations as provincial governments, businesses, universities, and provincial police forces. Secondment arrangements with other agencies should be approved by the Minister.

Career paths

73. Like most police forces in Canada and in other western countries such as the United States and the United Kingdom, the R.C.M.P. has adopted a 'generalist' approach in developing the careers of its members. Regular members are not encouraged to become specialists. Rather, after spending two or three years in one type of policing, they are often transferred by the Force to another geographic location, often to assume quite different duties. Nor is it unusual to find members who, after spending all of their careers in operational roles, are appointed to an administrative job, for example in the personnel or financial area.

74. Here is the actual career path of an inspector now serving in the Security Service, who has been with the Force since 1959. It may well be typical.

10 months	— recruit training in Regina (this is now 6 months)
2 years, 9 months	— general detachment duties first in Prince Rupert, B.C. and then in Terrace, B.C.
2 years	— highway patrol duties in Ottawa
1 year	— Security Service - counter-subversion branch in Ottawa
3 years	— university training at Carleton University, Ottawa, (summers spent in counter-espionage and counter-subversion in Ottawa)
4 months	— security screening duties in Ottawa
5 years	— counter-espionage branch in Ottawa
1 year	— research role, first in central research branch, then in counter-espionage branch in Ottawa
5 years	— personnel administration role in Ottawa

75. The inappropriateness of the Force's generalist career model was a recurring criticism among Security Service members. The problems identified are of three kinds. First, needed continuity is not built up and maintained in areas requiring in-depth knowledge and experience. Second, a significant

number of people in the Service are doing jobs they do not enjoy. And third, people in the Service appear to be less willing to move their families as often as the generalist career model dictates.

76. The Security Service conducted a detailed study of two of their largest branches to document some of these problems more fully. This study confirms that Security Service employees change jobs frequently; the Tables below summarize the results.

Table 6

Percentage of Branch employees (not including Support Staff) who changed jobs

	Branch 1	Branch 2
1975/76 (12 months)	56.3	33.8
1976/77 (12 months)	44.9	54.1
1977/78 (12 months)	68.2	47.9

Table 7 gives an idea of how devastating this type of movement can be on job continuity.

Table 7

Effects of Movement on Job Continuity 1975/78

	Branch 1	Branch 2
Percentage of total branch employees remaining in the Branch for the 3-year period 1975/78	23.1	21.6
Percentage of total branch employees remaining in the same job over the 3-year period 1975/78	6.2	6.8

The extent of the movement within the Service and the resulting lack of job continuity, as illustrated by the above Tables, is extremely harmful to the effectiveness of the Security Service. It also has a bad effect on the morale and well-being of employees and, consequently, on their families.

77. Other government departments, facing somewhat similar problems, have adopted approaches that may be worth emulating. External Affairs, for example, has attempted to create 'broad' specialties. Each foreign service officer, at some point early in his or her career, chooses two such specialties — usually one of these is a functional specialty (for example, economics), and the other a geographic specialty (perhaps Southeast Asia). This broad specialties notion could be modified and applied to the Security Service. One such specialty could be East Bloc countries, resulting in a career path, something as follows:

2 years in H.Q. in Counter-espionage Branch

3-4 years as an analyst in a regional office

3-4 years in H.Q. in Counter-espionage Branch

1-2 years as a liaison officer in a European country

1-2 years secondment to another government department with an interest in East Bloc relations

several more years in Counter-espionage Branch.

78. Some intelligence officers may join the agency without a specialty in mind. These individuals might embark on a career path which would expose them to a variety of work experiences in the early years of their career. Following this period when they are 'generalists', their careers should be built around a specialty or specialties. The high frequency of transfer from one area to another must be avoided in the new agency if a satisfactory level of effectiveness is to be achieved by taking advantage of specialization. Specialization may allow an intelligence officer to obtain employment more easily outside the agency, thus avoiding the problems associated with an employee being locked into his employment.

79. Implicit in an approach stressing greater specialization is the need for an improved career-planning capability — a capability which does not exist within the Security Service at the present time. Moreover, we believe that such a career-planning capability can function only with the close collaboration and support of those in operational jobs, who should be involved in both the design of this new career-planning approach and its implementation.

80. An implication of more specialized career paths is that not all those in research roles within the agency would have to become investigators at some point in their career, or vice versa. In our view, these functions, while they both have an analytical component, are different and consequently attract people with different skills and inclinations. Some investigators and researchers might profitably exchange roles, but the agency should not build its staff on the assumption that all members are generalists who can move from role to role every two or three years and be proficient in each area. What the agency must pay very close attention to, however, is how the researchers and investigators coordinate their work. It would be very damaging for two distinct streams to develop within the agency — one for 'thinkers', and another for 'doers'.

81. Besides adopting a more specialized approach to career planning, there are at least two other ways in which the security intelligence agency can enhance job continuity in key areas of its work. The first is to reduce the number of job levels within the organization. There are currently nine levels of regular members, ranging from constable to Director General, within the Service. Special constables and civilian members below the rank of constable would add to this total. What we suggest is reducing the number of levels, perhaps to five or six. This change would have several advantages. It would allow incumbents to remain in a position for longer periods and, at the same time, receive successive pay raises. (By reducing the number of levels, the pay band for each level will widen.) In addition, reducing the number of levels will also tend to 'flatten' the organizational pyramid, and this flattening should facilitate better communication within the agency. The Church Committee Report made a similar comment about the large number of bureaucratic layers in the C.I.A., and the resulting filtering problems as information moved up the organizational pyramid, often losing something at each level. As the Committee noted, ". . . there are too many people writing reports about reports."[11]

[11] United States Senate, *Final Report of the Select Committee to Study Governmental Operations*, Book I, p. 269.

82. Another approach that will help to provide opportunities for more specialization and job continuity is to create a number of senior positions throughout the agency which do not have heavy administrative responsibilities. Currently within the Security Service, a promotion invariably means accepting responsibility for managing more people. Thus, it is difficult for senior people within the Service to develop any degree of specialized knowledge. As an example of what we are proposing, the agency might establish several senior analyst positions in the counter-espionage area with no administrative responsibilities. Experienced analysts could be promoted to these jobs without loss of continuity and without wasting the specialized knowledge they have built up.

Training and development

83. A description of the training and development opportunities available to Security Service members must begin with the recruit training which a regular member receives on first joining the Force. Since 1969, all recruit training has been done at the R.C.M.P.'s Regina Academy. The course lasts for six months and costs approximately $18,000 per recruit. Following completion of this course, a new recruit is given an additional six months on the job training at a regular Force detachment.

84. The Regina Academy relies mainly on instructors who are regular members from operating divisions, and who come to Regina for a three-year period. Outside resource people are employed as instructors as well, but they teach less than 6% of the formal periods. The curriculum is a mixture of physical conditioning and academic subjects encompassing some 858 formal periods. (One of the officers at the Academy told us that the average student would work approximately 75 hours per week.) About half of these formal periods are devoted to the academic side of recruit training, made up of law, human relations (history of policing, human behaviour, criminal justice system, and effective speaking), operational techniques (typing, report writing, care and handling of prisoners), and technical devices (fingerprinting, photography and so on). The other half of the curriculum is more physically oriented — driver training, drill, physical training, self-defence, swimming, and small-arms training. Equestrian training is no longer given at the Regina Academy. Training in the law is only a small part of a recruit's curriculum, accounting for approximately 15% of the formal periods of instruction.

85. According to the non-commissioned officer in charge of the academic section, the Academy employs a "systems approach" to training. This approach is one behavioural psychologists would feel comfortable with. Trainers define as precisely as possible "terminal behaviours" or "end of course behaviours". These desired behaviours provide the basis for building course standards, deciding on teaching methodologies, and evaluating the effectiveness of courses. To be useful, these "terminal behaviours" have to be specific and concrete — for example, "identifying traffic violations", or "understanding criminal trial procedures". Using less technical language, the officer in charge of the Academy gave us a similar explanation of the underlying philosophy of recruit training. Of all the training available to a member, he noted, recruit training is perhaps the most critical "... in terms of molding the new member

in the image of the Force." Another senior officer at the Academy emphasized the importance of barracks living as an ingredient in recruit training. The effect of living at close quarters with 31 others, all of whom are enduring the same demanding activities, is, he explained, to create a surrogate family for a new recruit.

86. Once a regular member enters the Security Service, the bulk of his training occurs within the Service itself until he reaches the senior officer levels. Before 1945, members of the Security Service received no formal training. The first formal course was given in 1947 when members were provided with a series of lectures related to their investigative duties. By 1979, the Security Service's Training and Development Branch offered four major courses:

— *Intensive Basic Parts I & II*, which are aimed at newly appointed analysts and investigators.

— *The Intermediate and Senior Courses*, which are management oriented, and aimed at N.C.O.s, junior officers and their equivalents. These courses are each of two weeks duration.

The legal content in these courses is limited. In the Intensive Basic Course, there is one session of two hours devoted to the legal basis of the Security Service. This same session was added to the Intermediate Course in the fall of 1978.

87. Three new courses have been under development during the life of our Commission and will likely be operational when this Report is published. The first is a new induction course for those entering the Security Service who are not eligible for the Intensive Basic Course. The second new course about to be offered is aimed at improving analytical skills. The assumption behind the course is that although analysts are 'born not made', a course can improve analytical skills by exposing people to analytical tools such as critical-path diagramming and data-collation techniques. Finally, the Training and Development Branch, with the cooperation of the R.C.M.P. Legal Branch, is developing a more intensive 15-hour course on legal issues relevant to the Security Service. The aim is to present this course to all area commands.

88. The 18 staff members of the Training and Development Branch rarely teach courses. Rather they are course 'coordinators' who rely on resources both within and outside the Security Service to do the actual teaching. In 1979, five of these 18 staff members had university degrees. Few, if any, had any teaching experience prior to coming to the Branch. In addition to this Headquarters staff, there are full-time training personnel in Ottawa, Toronto and Montreal. Other area commands have staff members in part-time training capacities.

89. In addition to developing new in-house courses during the last decade, the Security Service began placing more emphasis on sending members to university on a full-time basis or subsidizing part-time university attendance. Table 8 demonstrates this trend.

Table 8

Year	Number Graduated from Full-Time University	Year	Part-Time University Attendance
1969	5	1972/73	257
1970	2	1973/74	544
1971	13	1974/75	491
1972	10	1975/76	412
1973	17	1976/77	486
1974	19	1977/78	311
1975	19	1978/79	336
1976	17	1979/80	437
	102		

90. We are favourably impressed with some aspects of the current approach to Security Service training. The greater emphasis now being placed on discussing legal issues is one example. Another is the Branch's identification of its future priorities: the more systematic development of on-the-job training and development; improving post-course follow-up to assess changes in the work performance of trainees; and the introduction of operational training at more senior levels.

91. Nonetheless, we believe significant changes are required in this area of personnel policy. A number of these changes flow from earlier recommendations, which called for a more experienced, more mature, and better educated person, who would enter the agency at a variety of levels. Thus, the current introductory course for analysts and investigators (the Intensive Basic Course) should be substantially modified. The emphasis should be on developing a much more sophisticated skill in dealing with the legal, political and moral contexts of security intelligence work and mastering 'tradecraft' techniques. Similarly, the existing six-month R.C.M.P. recruit training programme at Regina is inappropriate for those individuals wishing to work for a security intelligence agency. There is too much emphasis on 'parade square' discipline and on molding behaviour, and the course content is understandably oriented to police work rather than to the more specialized and politically oriented aspects of security intelligence. Finally, we find many of the aspects of the Regina programme authoritarian in tone, and likely unacceptable to the range of university graduates from which we think the security intelligence agency should draw many of its recruits in the 1980s.

92. The training and development programmes also reflect a general tendency within the Security Service towards insularity. We propose a variety of training approaches that will counteract this tendency by constantly exposing its members to ideas from persons outside the agency. We have the following approaches in mind: relying more on outside advice about curriculum, particularly in the areas of law, management, and the social and behavioural sciences; designing training experiences that will combine security intelligence members with people from other departments to examine areas of common concern (e.g. the covert intentions of a particular country); having intelligence officers attend two- to six-week management courses, especially designed by certain universities for middle and senior managers in the private and public sectors; and developing a security intelligence course aimed at an international audience of 'friendly' agencies.

93. We voice one note of caution concerning future efforts of Canada's security intelligence agency to collaborate with foreign agencies in developing training programmes. The mandates of these agencies may differ markedly from that of the Canadian agency. Consequently, collaboration runs the risk of introducing to Canadians a set of ideas and techniques which, if applied, could be outside the Canadian agency's mandate. Cooperation with foreign agencies on training should not be approached lightly. As we recommended in an earlier chapter on the international dimensions of the Security Service's work, exchange of personnel for training courses should be part of the agreement drawn up between Canada's security intelligence agency and foreign agencies with which it co-operates. In addition, the Minister should be informed when training exchanges actually occur.

94. Finally, as in other important areas of personnel policy, managers in operational branches should play a more active role in the design of training programmes and in their implementation. Furthermore, while it is important to continue to recruit people with operational experience into training roles, this should not be the exclusive means of staffing this function. Training and development personnel, like others in the security intelligence agency, can benefit from increased specialization.

Unionization

95. Until recently, members of the R.C.M.P. (the "member" category does not include public servants) did not appear to have the right to unionize. The R.C.M.P. Administration Manual, which derives its authority from subsection 21(2) of the R.C.M.P. Act, provided that a member could not

> Engage in activities which involve joining a union, association or similar collective bargaining group.

This prohibition has been rescinded but other restrictions on collective bargaining in the R.C.M.P. are also found in the Public Service Staff Relations Act.[12] That Act is the central piece of legislation governing collective bargaining in the federal public sector. The Act applies generally to all the Public Service, but expressly excluded from the provisions of the Act is

> . . . a person who is a member or special constable of the Royal Canadian Mounted Police or who is employed by that Force under terms and conditions substantially the same as those of a member thereof. . . (Para. 2(e)).

Thus, non-member (Public Service) employees of the R.C.M.P. Security Service have the right to bargain collectively under the Public Service Staff Relations Act, but not those employees who are regular, civilian or special constable members of the Force. There has been no test in the courts as to whether other legislation in the field of labour relations would permit a group of R.C.M.P. members to be certified as a union and to acquire collective bargaining rights. That possibility therefore remains uncertain.

96. The R.C.M.P. does have a "Division Staff Relations Representative Programme" which allows the R.C.M.P. member some participation in management decisions that affect him. The members of each division elect a

[12] R.S.C. 1970, ch.P-35.

full-time representative "... to present problems, concerns and recommendations on behalf of the members to management". The R.C.M.P.'s Administration Manual under Chapter II.16, provides:

> The Division Staff Relations Representatives will participate in the decision-making process whenever practicable, i.e., Headquarters benefits studies; pay discussion; kit and clothing design; division boards on transfers and promotions; succession planning; grievances and all meetings where policy directly affecting the welfare, dignity and operational effectiveness of the members is being discussed.

97. We believe it is imperative that members of a security intelligence agency should not be allowed to unionize. Indeed, we would extend this prohibition to cover public servants who are now employees of the R.C.M.P. Security Service. We base this recommendation on internal security considerations. Union negotiations involving a security intelligence organization run the risk that information of considerable value will become known to a foreign intelligence agency — information such as the number of employees, their duties, the command structure of the agency, and recruiting practices. In addition, we worry about the possibility of union-management relationships becoming so embittered that the risks of damaging leaks of information, or even an enemy penetration, become unacceptably high.

98. As an alternative to granting unionization rights to agency employees, we propose the following three-point approach. First, the security intelligence agency should fashion a managerial style which stresses employee participation in decision-making. (We shall describe such a style in more detail in a later section of this chapter.) Secondly, the agency should encourage the formation of an employee association which would make representations to the management of the agency with respect to salaries and working conditions. This association would provide another means for allowing employees to communicate with the management of the agency and to influence important decisions of the agency. We see this association playing only a secondary role in ensuring good management/employee relations. The more successful the agency is at establishing a participatory management style, the less important the role of this association will be in that regard. Finally, the salary and benefits of agency employees should be tied to those of the Public Service of Canada through a pre-determined formula. This arrangement will ensure that agency employees receive at least the major benefits of the collective bargaining process.

Agency employees and the Public Service of Canada

99. We now consider the question whether or not agency employees should belong to the Public Service of Canada as defined by the Public Service Staff Relations Act. We believe it essential that agency employees not belong to the Public Service. By virtue of section 5 of the Public Service Employment Act, the Public Service Commission has the authority to appoint and dismiss public servants. Given the special nature of the threat of penetration facing a security intelligence agency, we believe strongly that the agency itself, rather than the Public Service Commission, should have this authority. The agency requires the flexibility to develop a more stringent set of screening procedures for its employees than those pertaining to the Public Service. Conversely, it also

requires a less stringent set of conditions for releasing an employee for security reasons. We know of no security or intelligence agency which does not have the authority to hire and dismiss its own employees.

100. A major disadvantage of agency employees not belonging to the Public Service is that movement of personnel between the agency and federal government departments will be more difficult to effect. We propose several ways to reduce this disadvantage. To facilitate the transfer to and from the Public Service, staff benefits for agency personnel should be similar to those enjoyed by federal public servants. Furthermore, the benefits should be 'portable' between the agency and the federal government, and should be covered by portability arrangements between the federal government and private sector organizations and other levels of government. Finally, we propose that agency employees have the same rights now enjoyed by members of the R.C.M.P. and the Canadian Armed Forces,[13] who, for the purposes of being eligible to enter Public Service competitions, are deemed to be persons employed in the Public Service. Such a provision would also facilitate movement from the agency to the Public Service.

Counselling

101. Estimates of the portion of any employee group suffering from emotional problems severe enough to affect job performance range as high as 15 per cent. Emotional problems can be triggered by a variety of causes — marital difficulties, alcoholism, physical sickness, or job-related factors. In a 1977 study of R.C.M.P. health services, the author, Dr. M.L. Webb, gave evidence illustrating that Force employees, and, in particular, certain categories of Security Service employees, have more significant stress problems associated with their work than the average population.

102. Troubled employees are a significant cost to any organization, in shoddy work, serious mistakes, high rates of absenteeism, danger to other employees in certain cases, and in the expense of hiring and training replacements. For an intelligence agency, however, there is the added danger of penetration. Emotionally troubled employees may become prime targets for agents of unfriendly foreign intelligence organizations, who are highly trained in both detecting and exploiting such employees. Given the serious consequences of such a penetration, it is not an unreasonable expectation that a security intelligence agency would be highly skilled at dealing with this type of problem.

103. During the interview programme that our staff conducted of some Security Service employees, most interviewees were unfamiliar with the term 'counselling' and were not fully aware of what programmes existed within the Security Service. One participant who was aware of existing programmes called them "primitive". Another described them as "fragmented".

104. One approach to employee counselling, which has been adopted by a number of organizations both in the private and public sector, involves the hiring of staff especially trained in counselling to help emotionally troubled employees. The success of such a programme in a security intelligence agency would appear to depend upon several factors. The programme should for the

[13] Under section 2(2) of the Public Service Employment Act.

most part be voluntary. In addition, confidentiality must be maintained. Only in exceptional circumstances should those in counselling roles report information about employees which has been received in confidence. Two such exceptions, of which employees should be aware, are information about participation in illegal acts, and information given to counsellors which suggests that there is a serious risk of penetration by hostile intelligence agencies.

105. We note that Dr. Webb, in the study we referred to above, recommended a similar programme for the Force as a whole. The Force has accepted this recommendation and, subject to Treasury Board approval, plans to implement it in the fiscal year 1981/82.

Grievances

106. Like many organizations, the R.C.M.P. has both a formal and an informal means of dealing with employee grievances. The 1976 Report of the Commission of Inquiry Relating to Public Complaints, Internal Discipline and Grievance Procedure Within the R.C.M.P. (commonly known as the Marin Commission) strongly supported informal approaches for dealing with grievances, prior to resorting to more formal means:

> ... we strongly approve of the current practice of seeking local and informal avenues of resolution of grievances before resorting to formal procedures. In our view, this practice should be encouraged and strengthened wherever possible as it constitutes the most efficient method of resolving grievances.[14]

107. We concur with the Marin Commission's emphasis on informal approaches and believe that this philosophy should be adopted by a security intelligence agency. Indeed, senior managers within the agency should closely monitor the use of more formal grievance procedures. A rising number of formal grievances is a likely indicator of a problem area — recruiting errors, poor internal communications, an autocratic managerial style, or insufficient supervisory training programmes.

108. The current R.C.M.P. formal grievance procedure involves a four-stage process, starting with the officer commanding a subdivision and moving up through the Force hierarchy to the Commissioner. We do not think that such a cumbersome process is required for a security intelligence agency. We favour a simpler two-stage procedure. The first stage would involve submission to a three-member grievance board appointed by the Director General. The board would investigate the grievance, hear the parties concerned, and make a ruling. The second stage would be an appeal procedure, whereby any of the parties to the grievance could ask the Director General, or a deputy appointed by him, to review the Board's decision. Following the Marin Commission (and current R.C.M.P. policy) we propose that no member should be penalized directly or indirectly as a result of lodging a grievance.

Remedial action for improper behaviour

109. The R.C.M.P.'s approach to improper conduct on the part of its members continues to reflect the origins of the Force — a paramilitary

[14] *The Report of the Commission of Inquiry Relating to Public Complaints, Internal Discipline and Grievance Procedure Within The R.C.M.P.*, 1976, p. 182.

organization with responsibilities for frontier policing. As the Marin Commission report stated, "Discipline within the R.C.M.P. was developed and has evolved under the influence of the military character of the Force and the operational requirements of law enforcement."[15] The Force originally relied on the rules of discipline of the Royal Irish Constabulary, which, in turn, duplicated many of the military procedures in use in England and Canada at the time. The Force was also originally staffed with men who served as officers and non-commissioned officers in the Canadian Militia and the British Army.

110. "Police service on the frontier", explained the Marin Commission Report, "required that the majority of the members of the Force serve independently or in groups of two or three, far removed from direct supervision. Given the authority and discretionary power of a police officer, it was imperative that he exercise self-discipline and self-control".[16] But balancing the Force's trust that its officers would exercise self-restraint and control were "provisions which exemplified a strict and summary approach to breaches of discipline". The Report went on to note that minor misconduct by a member of the Force "constituted more than a misdeed; it gave evidence of a breach of trust and characterized the member as unreliable. When self-discipline failed, punishment was swift and severe".[17]

111. Sections of the R.C.M.P. Act establishing the penalties for serious offences are an indication of the potential harshness of the current approach to improper behaviour. Penalties for major service offences — for example, refusing to obey the lawful command of a superior — range from a year's imprisonment, to a fine not exceeding $500.00, to a reduction in rank, to a reprimand. For minor service offences, — for example, immoderate consumption of alcohol or using profane language, — punishment ranges from confinement to barracks for up to 30 days to a simple reprimand.

112. In addition to being unduly harsh, the current disciplinary system of the R.C.M.P. is characterized by a multitude of regulations governing the conduct and performance of members. The impression is one of a great web of rules touching every facet of a member's on-duty life and many parts of his private life. Moreover, the process of determining disciplinary steps is laid down in great detail and tends to be very adversarial in nature. Thus, there are procedures for launching an investigation, for laying of service charges, for formal quasi-judicial hearings to determine the member's culpability, for determining penalties, and finally for appealing the verdict.

113. The Marin Commission Report was highly critical of the present disciplinary system of the Force. The Commissioners found the procedures too formal, the control too centralized, the member's rights ill-defined, and the exercise of disciplinary authority too arbitrary. We concur with these criticisms. That such a system should still exist in the latter part of the 20th century, and that the impetus for changing it had to come from an outside body like the Marin Commission, are additional evidence of a weakness in the managerial expertise existing within the Force. Bill C-50, An Act to Amend

[15] *Ibid.*, p. 111.
[16] *Ibid.*, p. 31.
[17] *Ibid.*, pp. 111-112.

the Royal Canadian Mounted Police Act, which was introduced in April 1978, and which would have substantially modified the Force's disciplinary procedures along many of the lines recommended by the Marin Commission, died on the order paper.

114. The approach for dealing with improper behaviour which we recommend for the security intelligence agency is a system based on a different set of philosophical principles. First, we believe that the cornerstone of such a system should be self-discipline and self-control, based on more positive motivations than fear of punishment. The great majority of employees will exercise a high degree of self-discipline and control if they have taken an active part in working out with their superiors the conduct and performance expected of them, or are in very substantial agreement with the standards because of a thorough understanding of the need for the standards. We shall be developing this theme much more fully in the next section of this chapter. Here we want to emphasize that the collegial management style we are recommending is not in any way incompatible with a highly disciplined security intelligence agency which acts legally, properly, and in concert with government policies. Quite the contrary, collegiality can and should be structured in such a way that security intelligence officers 'going off on their own' in disregard of government and agency policies, is simply not tolerated within the agency.

115. Second, primary emphasis on correcting inappropriate behaviour should be through remedial action, rather than by punishing individuals. Moreover, the remedial action may not be directed solely or primarily at individuals. Rather, improper behaviour may indicate faults in certain organizational practices: communication may be poor, supervisory patterns inadequate, or training programmes too skimpy. When remedial action is directed toward individuals, the key, in our view, is to avoid a highly formalized adversarial process. Supervisors may need to rely on expert staff resources to help them work out remedial programmes with certain employees. The stress should be on creatively working out joint solutions to problems rather than on punishing people. Only in rare circumstances should formalized disciplinary procedures be launched against an employee.

116. We propose one important exception to the above approach: where there is evidence of an illegality on the part of an employee. The procedure to be followed in handling such cases is described in Part V, Chapter 8. The employee should be suspended with pay, pending the outcome of this procedure.

117. In a few extreme cases, the best solution may appear to be dismissal. Such a decision should not be made lightly and it should be made only after supervisors and others have made considerable effort in applying remedial measures. The actual decision should be made by the Deputy Solicitor General, on the advice of the Director General and his senior management team. The Director General may wish to consult others outside the agency, both to test the soundness of his recommendation to dismiss an employee and to explore possible employment options for the individual elsewhere. As in most other private and public organizations, the decision to terminate employment should be based on 'cause'. In some instances, it may be appropriate for the agency to

pay the costs of a termination counsellor for the employee and to make a sustained effort to help the dismissed employee find suitable work elsewhere. Avoiding the problems of disgruntled ex-employees of the security intelligence agency will be well worth the effort as such persons can do great harm to a country's security system.

118. We should make one other point about dismissal procedures. That concerns dismissals based on security grounds. The dilemma here is that the Director General must tolerate a much lower level of risk than would the heads of most other government departments and agencies, and yet, at the same time, individual employees must have some sense of job security upon agreeing to work for the agency. There are no easy answers here. The best approach we can think of is as follows. The Director General should have the power to suspend a person with pay while a security investigation is conducted. If the evidence would not warrant dismissal from another government department and yet leaves some doubt as to the employee's reliability within a security intelligence agency, then the employee should, if possible, be given work of comparable status in a non-sensitive area in another federal government agency or department. The Director General should work out a procedure for handling such cases and seek the approval of the appropriate interdepartmental committee.

WE RECOMMEND THAT the security intelligence agency adopt the following policies to help it determine who should work for the agency:

(a) the agency requires staff with a wide variety of backgrounds in governmental, non-governmental, and police organizations;

(b) police experience should be a prerequisite for only a small number of specialized positions;

(c) the agency should periodically hire persons from outside the agency for middle and senior management positions;

(d) having a university degree should not be a prerequisite for joining the agency. Nonetheless, the agency should actively recruit those with university training;

(e) the agency should hire individuals with training in a wide variety of academic disciplines;

(f) the agency should seek employees with the following characteristics: patience; discretion; emotional stability; maturity; tolerance; no exploitable character weaknesses; a keen sense of, and support for, liberal democratic principles; political acumen; and the capacity to work in an organization about which little is said publicly.

(74)

WE RECOMMEND THAT the security intelligence agency adopt the following recruiting procedures:

(a) it should widen its recruiting pool in order to attract the type of personnel we have recommended, rather than rely on the R.C.M.P. as its primary source of recruits;

(b) apart from support staff, it should have only one category of employee, to be known as intelligence officers. Intelligence officers should not be given military or police ranks;

(c) it should not rely primarily on referral by existing or former employees to attract new recruits but rather should employ more conventional methods, including recruiting on university campuses and advertising in newspapers;

(d) in addition to the personnel interview, it should develop other means, such as psychological testing and testing for writing and analytical ability, to ascertain the suitability of a candidate for security intelligence work;

(e) it should involve experienced and senior operational personnel more actively in the recruitment process.

(75)

WE RECOMMEND THAT

(a) the security intelligence agency initiate a more active secondment programme, involving federal government departments, the R.C.M.P., provincial police forces, labour unions, business, provincial governments, universities, and foreign agencies;

(b) secondment arrangements with foreign agencies should be approved by the Minister responsible for the security intelligence agency.

(76)

WE RECOMMEND THAT the security intelligence agency:

(a) develop an improved career planning capability in order to effect greater specialization in career paths;

(b) ensure that there is close collaboration between line and staff personnel in the design and implementation of specialized career paths.

(77)

WE RECOMMEND THAT the number of job levels for intelligence officers within the security intelligence agency be reduced.

(78)

WE RECOMMEND THAT the security intelligence agency establish a number of positions designed for senior intelligence officers who would have no administrative responsibilities.

(79)

WE RECOMMEND THAT security service training be redesigned so that it is more suitable for better educated, more experienced recruits. There should be less emphasis on 'parade square' discipline and 'molding' behaviour and more emphasis on developing an understanding of political, legal and moral contexts and mastering tradecraft techniques.

(80)

WE RECOMMEND THAT the security intelligence agency initiate a variety of training programmes with an aim to exposing its members to ideas from persons outside the agency.

(81)

WE RECOMMEND THAT

(a) managers in operational jobs take an active role in the design and implementation of training and development programmes;

(b) opportunities for increased specialization be available for training and development staff.

(82)

WE RECOMMEND THAT

(a) security intelligence agency employees not be allowed to unionize, and this be drawn clearly to the attention of each person applying to join the agency;

(b) the security intelligence agency

(i) adopt a managerial approach which encourages employee participation in decision-making,

(ii) encourage the formation of an employee association, and

(iii) tie agency salaries and benefits by a fixed formula to the Public Service of Canada.

(83)

WE RECOMMEND THAT

(a) employees of the security intelligence agency not belong to the Public Service of Canada;

(b) the employee benefits of the security intelligence agency be the same as those enjoyed by federal public servants;

(c) portability of employee benefits exist between the agency and the federal government;

(d) pension portability arrangements between the federal government and other organizations including other levels of government encompass the security intelligence agency;

(e) for the purposes of being eligible to enter public service competitions, employees of the security intelligence agency be deemed to be persons employed in the Public Service.

(84)

WE RECOMMEND THAT the security intelligence agency establish an employee counselling programme based on the two principles of voluntary usage and confidentiality of information given to the counsellors.

(85)

WE RECOMMEND THAT the senior management of the security intelligence agency

(a) emphasize the practice of seeking local and informal avenues of resolution of grievances before resorting to formal procedures;

(b) monitor carefully the use of formal grievance procedures as a possible indicator of problem areas in current personnel policies;

(c) establish a two-stage formal grievance procedure, involving a three-person grievance board at the first stage, and an appeal to the Director General at the second stage;

(d) ensure that no member be penalized directly or indirectly as a result of lodging a grievance.

(86)

WE RECOMMEND THAT the security intelligence agency develop a program for dealing with improper behaviour which

(a) emphasizes remedial action rather than punishment;

(b) requires the Director General, in the case of an alleged illegality, to suspend an employee with pay and to refer the case to the Solicitor General;

(c) places responsibility for dismissal with the Deputy Solicitor General, subject to the advice of the Director General and his senior management team;

(d) emphasizes the necessity of the security intelligence agency expending every effort, in appropriate instances, to help dismissed employees find new work;

(e) provides for a procedure for relocating employees who are suspected of being security risks to non-sensitive areas in other federal government departments.

(87)

D. APPROACHES TO LEADERSHIP, ORGANIZATION AND DECISION-MAKING

119. To this point, we have concentrated on describing the kind of people who should work in a security intelligence agency, and the appropriate set of personnel policies — recruiting, training, career paths, and so on — so that the 'right' people are doing the 'right' jobs. For some, this is the essence of good management: problems of effectiveness, propriety and legality simply will not arise as long as the organization has good people and keeps them productively occupied. Unfortunately, the management of an organization is more complicated than this view suggests. People who are exemplary citizens in their private lives — law-abiding, morally sensitive and public-minded — frequently find it extremely difficult to withstand organizational pressures either to participate or acquiesce in improper or illegal acts of other members of the organization. Thus it is important to examine those features of an organization which lead to illegalities and improprieties.

120. In this section, we examine two dimensions of management: leadership style, and some related principles of organization. The focus of both these topics is how people within a security intelligence agency relate to one another in making day-to-day decisions.

Leadership style

121. For many, the word 'leadership' conjures up images of strong-minded, clear-thinking individuals giving incisive orders. We shall leave it to others to argue whether such a leadership style is appropriate in any organization, even an army in battle. We can state with some certainty that such a style, with its reliance on obedience, is inappropriate for the kind of security intelligence organization we are proposing. The thoughtful, mature, well-educated individual who, we believe, is needed for security intelligence work is not likely to tolerate such a style. Moreover, advocates of this approach to leadership ignore an increasingly important aspect of modern organizations: they are complex and their parts are highly interdependent. To function effectively

within a security intelligence agency often requires getting things done by working with other people with whom no superior/subordinate relationship exists. In sum, a leadership style based on giving orders must give way to a team approach where the emphasis is on shared decision-making, and where control by superiors is largely replaced by self-control and self-direction, based on a common understanding of shared goals. This is not to argue that giving orders is never appropriate, only that there are often more effective means of getting things done.

122. A reading of the opening section of the Force's four-volume Administrative Manual would suggest that it is committed to the kind of leadership approach we have recommended above. Section 6 of the chapter on "The Principles of Policing and Management in the R.C.M.P." is as follows:

> 6. Police personnel at all levels should be given the opportunity to participate in the setting of goals and deciding the means of achieving them. Managers should set an atmosphere wherein they can carry out their responsibilities on the basis of mutual confidence, respect and integrity, without simply relying on their authority or position.

123. The evidence we have heard in our hearings, the numerous informal meetings we and our staff have had with members of the Force, and our examination of file material all suggest that this principle is not as widely followed within the Security Service, nor within the Force as a whole, as it should be. For example, the descriptions we have given in this chapter of current personnel policies in such areas as discipline and recruit training indicate an 'obey or else' philosophy of leadership which is at odds with the above principle. And consider this testimony from an officer in the Security Service:

> . . . we knew we were confronted, among other things, with severe. . . hierarchical authority problems. Younger members were very loath to express their honest opinion when their seniors were present, because if they were disagreeing with their seniors, some of whom thought we were in the best of all possible worlds. . . they would be told off.
>
> (Vol. 53, pp. 8620-8621.)

124. We have found some evidence that a team approach to decision-making is taken seriously within the Security Service. For example, we were impressed by recent developments in the Service's planning process, which has evolved into a well-integrated process offering opportunities for participation in planning and detailed target setting throughout the organization. And we have spoken to a number of officers who were trying to develop a more participatory approach in their units. Nonetheless, we believe considerably more progress in this direction is required throughout the Security Service. In particular more emphasis needs to be given in training courses to practising small-group decision-making techniques so as to support such a leadership style.

125. A review of Security Service files has illustrated the problems faced by a source and his Security Service 'handler' and gives a strong hint of the kind of filters which can develop in an organization — filters which can distort the flow of information to senior management. That such communication distortions should develop to reduce the effective operation of a security intelligence

agency affords sufficient grounds for concern. That such distortions could, in addition, keep from senior management information about existing or potential improprieties and illegalities is intolerable. The adoption of the leadership style we have advocated in this section — a style which assumes that conflict within an organization can be a positive stimulus provided it is faced openly and creatively — is one way to minimize the occurrence of communication problems within the agency. Creation of only one category of employee, a recommendation we made earlier in this chapter, is another means to achieve this end. In addition, there are other managerial policies which move in the same direction. For example, the agency should not have separate eating and social facilities for its various levels as is now the case in the R.C.M.P. In our view, such separate facilities tend to accentuate communication barriers within the agency. Moreover, senior management should develop regular opportunities for discussions with lower ranking employees whom they might not normally see in the course of their work.

126. Yet another device to facilitate communication is to encourage *ad hoc* groups established to examine particular problems, to include, when appropriate, staff from several management levels within the agency. Finally, when senior managers deal with the work of an individual, that person, however junior, should be present in the meeting where feasible.

Organizing principles

127. Most who work in large organizations are struck at some point by the inadequacy of an organization chart in showing how things really work. All employees, even at low levels, have working relationships with others in addition to their superiors, and these relationships shape and modify their own role and responsibilities to such an extent that behaviour within organizations cannot be described solely in terms of the formal organization chart. At middle and senior levels, interdependencies among organizational units become very pronounced and require managers to spend significant portions of their time working with others either 'across' the pyramid or belonging to another organization.

128. On several occasions in this and earlier chapters, we have recognized the importance of these interdependencies and recommended specific structures to deal with them. In our discussion of the security intelligence agency's mandate, we recommended the formation of a revamped O.P.R.C., whose composition would include both members of the security intelligence agency and others outside the agency, and whose function would be the review of proposals for 'full' investigations. In a similar vein, we have proposed that the Director General and his senior managers act as a team so that agency decisions may be tested against all the major viewpoints within the organization. These examples illustrate the importance we place on the security intelligence agency's conscious structuring of its key decision-making forums so that countervailing perspectives are brought to bear on important problems. The creative resolution of differences in viewpoint can produce decisions of high quality. There will be less likelihood of poorly considered operations and policies.

129. As a final illustration of this organizing principle of countervailling forces, we shall now consider how a security intelligence agency might go about developing and implementing policies relating to personnel matters. One of the dominant themes which arose in Commission interviews with R.C.M.P. personnel on personnel policies affecting the Security Service was the existence of a high degree of acrimony, tension and frustration in the relationship between those doing the operational work of the Service (i.e. those in 'line' jobs) and those responsible for Force-wide personnel policies (i.e. those in 'staff' jobs). Line personnel believed that those in staff positions lacked a proper understanding of Security Service work, were overly narrow and specialized, were too concerned with bureaucratic procedures and enforcing compliance, and, in general, were unsympathetic about helping line people solve some serious and pressing problems. Those in staff positions, on the other hand, tended to view line personnel as parochial, unconcerned with broader Force-wide interests, overly concerned with maintaining their independence, and guilty of a tendency to blame staff people for problems they should solve themselves.

130. The antipathy in this staff/line relationship has manifested itself over the last decade in a variety of ways which go beyond angry memos and long frustrating meetings. For example, we found several instances of outright non-compliance with certain personnel policies. An even more common phenomenon was the expenditure of large amounts of employee time in devising ingenious ways to get around or defeat certain policies (for example, Security Service branches putting forward numerous proposals for organization changes in order to deal with constraints imposed by the classification system). The situation we have described here is by no means unique to the R.C.M.P. Many organizations, both in the private and public sectors, experience a similar 'guerrilla warfare' between staff and line employees.

131. What can be done to minimize such problems? There appear to us to be a number of ways in which much closer collaboration can exist between staff and line components within a security intelligence agency. The most important is the recognition throughout the organization that developing and implementing personnel policies must be a joint responsibility of both line and staff managers. Moreover, there must be structures to reflect this sharing of responsibility. Responsibility for personnel policy should be vested in a senior committee composed of both line and staff managers. The advantage of this arrangement is that it begins to remove the staff personnel from an enforcement role, and yet provides them with a forum for exerting considerable influence on the direction of the organization's personnel policies. For line managers, such an arrangement means that they must become more active in thinking about and formulating personnel policies and consequently more committed to the end result.

WE RECOMMEND THAT the security intelligence agency develop

(a) a leadership style which relies less on giving orders and obedience and more on participation in decision-making, and

(b) training courses, especially in small group decision-making techniques, which will support such a leadership style.

(88)

WE RECOMMEND THAT, to minimize the likelihood of internal communication barriers developing, the senior management of the security intelligence agency should

(a) eliminate separate eating and social facilities based on job levels within the agency;

(b) develop a regular forum for communicating with staff they would not normally meet in the course of their work;

(c) encourage ad hoc problem-solving groups, when appropriate, to include staff from a variety of levels within the agency;

(d) encourage the attendance of junior ranking members when their work is discussed.

(89)

WE RECOMMEND THAT the security intelligence agency include in its key decision-making forums individuals who, because of their function, have different perspectives on the problems to be considered.

(90)

E. LEGAL ADVICE

132. An essential element in the structure of any government department or agency is its legal services. The part played by the legal adviser is more or less important depending on the role assigned to the department or agency. Because of the delicate and sensitive work to be performed by the security intelligence agency, as we have outlined it earlier in this part of our Report, and the potential for infringement of legal rights of individuals and organizations, it is of the utmost importance that the agency receive independent legal advice of the highest order and that it follow that legal advice scrupulously.

133. In the past the Security Service of the R.C.M.P. obtained its legal advice from the same sources as the rest of the Force, i.e. the Department of Justice or the Legal Branch of the R.C.M.P. In Part X, Chapter 3, we shall outline briefly the history of the Legal Branch of the R.C.M.P., and the current status and role of that Branch, and set out some recommendations for its future. Because we shall recommend a security intelligence agency separate from the R.C.M.P., we propose here to deal with how that separate agency should obtain its legal services.

134. For legal advice to be reliable, the lawyer providing it must be as free as possible from any external influence or pressures. This touchstone is a basic tenet of the legal profession. A lawyer must be free to express his opinion without fear that the content of that opinion might have an adverse effect on him personally. This principle applies equally to private practitioners and lawyers employed by the government. Recognition of this principle underlay the recommendations of the Royal Commission on Government Organization (1962) (the Glassco Commission). That Commission stated:

> Rotation of Justice lawyers into departments and back to the Department of Justice should bring a fresh touch of reality to the oft-times academic tone of Justice opinions and, at the same time maintain in the departments

the appropriate aura of neutrality required in rendering impartial legal advice.[18]

135. There are characteristics of a security intelligence agency which give a uniqueness to its legal requirements. Much of what it does is secret and in many cases very few people have any knowledge of its operations. Of even greater significance, most of the operations involve an intrusion into the lives of others which goes beyond what is normally encountered or permitted in our society. Earlier in this Report we defined the role of the agency and the powers that we think should be given to it. We also dealt with the mechanisms we think ought to be put in place to control the agency's activities. Underlying our recommendations is the principle that the agency must act within the law at all times. If the law is not adequate to allow the agency to perform its role it should seek to have the law changed. It should not under any circumstances knowingly or negligently break the law. This has two consequences for the legal services requirements of the agency. First, the agency requires legal advice, in advance, with respect to certain aspects of its operations to ensure that they are in conformity with the law; and second, it requires legal advice as to the best way to change the law if the law is not adequate to permit it to perform its assigned duties. We will now consider these two legal functions separately.

136. The secrecy associated with operations gives a particularity to the advice required. The 'need to know' principle, which we shall discuss in greater detail in a later section of this chapter, can result in a down-grading of the importance of questions of legality by those involved in the operations, who are not experts in the law and who may be facing a set of pressures to collect certain information. In addition, the number of people outside the agency having knowledge in advance of operations must be limited because of the risk of compromise of the operations. Any examination of the legalities of operations carried out prior to the execution of such operations must, therefore, be performed within the agency. We are strongly proposing to the government that the legal advisor be placed in a key position to advise on legal matters. The agency's legal adviser should be a member of the committee which authorizes the agency to use the full range of its investigative methods against a proposed target. The legal adviser should also examine each specific request for the granting of a warrant to perform an intrusive technique, so as to ensure that the application is in conformity with the law and the agency guidelines. Further, he should scrutinize specific proposals for using certain other investigative techniques to ensure that those proposals meet agency guidelines. As well as having a formal involvement in the approval process for sensitive operations, the legal adviser should be available to give advice in the planning of such operations, prior to the approval stage. Members at every level in the agency should be encouraged to consult with the legal adviser on all matters, with full candour. In this way, potential legal problems may be avoided and the morale of operational people will not suffer because of rejection of their proposed operations at a later stage due to legal considerations. The advice of

[18] *Royal Commission on Government Organization*, Queen's Printer, Ottawa, 1962, Vol. 2, p. 420.

the legal adviser as to the legality of an operation must be binding on the agency unless a contrary opinion is given by the Deputy Attorney General of Canada. Any knowledge by the legal adviser, either before or after the fact, of any illegal act by the agency must be reported by him to the Deputy Attorney General of Canada.

137. The second requirement of the agency for legal advice as to how inadequate laws ought to be changed, while in some respects similar to the provision of such advice to any government department or agency, again has some aspects unique to a security intelligence agency. The agency's legal adviser requires a detailed knowledge of the agency's operations and techniques to ensure that legislation which is drafted does not destroy the efficacy of the agency's clandestine activities. Later in this Report we shall be recommending that there be a special group of parliamentarians who would be kept informed by the government with respect to security matters. The details and reasoning behind some of the more sensitive aspects of legislative changes would be one of the areas in which they would be so informed. In this area of legislative change the legal adviser should counsel senior management of the agency in its dealing with Ministers, senior officials in other government departments and Parliamentary Committees, but he should not become the advocate for the agency. Such a role would be consistent with the role played by Department of Justice lawyers in other departments and agencies of the government.

138. In our opinion the legal advisers of the agency must be intimate with all aspects of the agency's activities. This means that they must have several years of continuous association with the agency. Because of the degree of secrecy required we consider it advisable that such lawyers attempt to handle as much as possible of the legal work without reference to any 'outside' lawyers. For the reasons mentioned previously about the benefits accruing from independent legal advice, we think that the legal advisers to the agency should be members of the integrated legal service of the Department of Justice. Since there will be little or no review by other lawyers of the legal advice given by the agency lawyers in advance of the execution of operations, it is imperative that such lawyers be well-qualified and of mature judgment. We think it would not be wise for a lawyer to make a career of being a legal adviser to the agency; however, we think it would be reasonable to expect that any lawyer spend from five to ten years in such a position. Obviously, he must be housed at the security intelligence agency's Headquarters and must be in full-time attendance there. The clear danger in these circumstances is that if he were to consider it a lifetime career, notwithstanding that he is a member of the Department of Justice, he might tend to lose his independence, either by being co-opted to the agency's way of thinking through long-term association, or because his career would be dependent upon the approval of him by the senior management of the agency. For this reason we think that there should be a limit on the duration of his services.

139. Until recently, one member of the Legal Branch of the R.C.M.P. worked full-time advising the Security Service of the R.C.M.P. In addition, much of the time of the Department of Justice lawyer assigned to the

R.C.M.P. was taken up with Security Service matters. (In Part X, Chapter 3, we discuss recent developments concerning the R.C.M.P.'s Legal Branch.) We are sure that more than one lawyer will be required by the security intelligence agency, and no doubt over time a system of staggering the appointments could be worked out which would ensure that there would always be one lawyer available in the agency who would be experienced in its work.

WE RECOMMEND THAT the legal services of the security intelligence agency be provided by the Department of Justice, and that the Department of Justice assign to the security intelligence agency well-qualified lawyers of mature judgment in sufficient number to provide all of the legal services required by the agency.

(91)

WE RECOMMEND THAT the lawyers assigned to the agency serve from five to ten years in that assignment and that there be a gradual staggering of the appointments so as to ensure that there is always at least one lawyer at the agency with several years' experience in its work.

(92)

WE RECOMMEND THAT the agency's legal advisers provide the agency with advice on the following matters:

(a) whether actions are in conformity with the law and agency guidelines;

(b) the legality of each application for a warrant to perform an intrusive technique and whether such application is in conformity with those agency guidelines with respect to its use;

(c) whether a proposal to use certain other investigative techniques is in conformity with the agency's guidelines.

(93)

WE RECOMMEND THAT the advice of the legal adviser be binding on the agency unless a contrary opinion is given by the Deputy Attorney General of Canada.

(94)

WE RECOMMEND THAT the legal adviser report to the Deputy Attorney General of Canada any knowledge he acquires of any illegal act by any member of the agency.

(95)

WE RECOMMEND THAT the legal adviser counsel senior management of the agency in its dealings with senior officials, Ministers or Parliamentary Committees with respect to the proposed legislative changes affecting the work of the agency.

(96)

F. INTERNAL AUDITING

140. The R.C.M.P. defines audits as "official systematic examinations" to "... assure senior managers that their policies are being observed". The practice of having audits conducted throughout the Force by a group on behalf of the Commissioner began in 1953. By the summer of 1977, an Audit Branch with three units — a Management Audit Unit, Financial Audit Unit, and an

Administration and Personnel Audit Unit — was in place. The officer in charge of this Branch reports to the Commissioner. Following the revelations which gave rise to this Commission, Commissioner Simmonds and the Solicitor General, Mr. Fox, announced the formation of an Operational Audit Unit, which was added to the Audit Branch in early 1978. Unlike the other units in the Branch which have Force-wide responsibilities, this latter unit focusses solely on the Security Service. In addition to the four audit units which form the Audit Branch, the Security Service has its own audit unit, which began its first audit in May 1978. Of these five audit units, three are important for our purposes — the Management Audit Unit and Operational Audit Unit in the R.C.M.P.'s Audit Branch and the Security Service's own audit unit.

141. The Management Audit Unit is the largest unit within the Audit Branch. In 1979 it had a complement of 14 full-time regular members — 2 Superintendents, 2 Inspectors, and 10 Staff Sergeants. The objective of the unit is to "assist all levels of management in the effective discharge of their responsibilities". To do this, the unit examines among other things the following: the use made of resources — personnel, financial, material; administrative and operational efficiency; internal control mechanisms; quality of communication; and morale levels. This unit completed an audit of the Security Service in 1976 and another in 1979. The aim is to have these audits done eventually on a two-year cycle.

142. The Operational Audit Unit, established in early 1978 by the Solicitor General and the Commissioner, has a mandate to examine all aspects of the Security Service to ensure that its activities are

(a) legal;

(b) within the mandate of the Security Service;

(c) consistent with Force policy;

(d) ethical and morally acceptable, and

(e) efficient and effective.

This unit has four full-time staff members — a Chief Superintendent, a Superintendent and two Staff Sergeants. Commissioner Simmonds, in testimony before us, explained the rationale for establishing this unit. The Security Service, unlike the other geographically based divisions within the Force, is both a policy centre and an operations centre. It does not have a number of Headquarters-based policy directorates 'riding herd' over it as do the other divisions. Hence, Commissioner Simmonds felt the need for ". . . a small audit team that reports directly to me and looks at the operations of the Director General, because my responsibilities are large and I am busy and I can't be spending every day looking at what he is doing..." (Vol. 164, p. 25188). The unit is authorized to have unrestricted access to Security Service files, but is not allowed to contact other agencies, police forces, or foreign governments. It began its work by auditing several of the Headquarters branches in a very extensive manner. In auditing the one operational branch, for example, the auditors looked at over 700 files at the outset, choosing some randomly and others by asking for specific policy files and sensitive operational files. After

this file review, they then conducted a number of interviews. This audit took a long time, some seven months, to complete. The audit of another Headquarters branch took close to four months. The heavy emphasis on file review is in contrast to the management audit, which relies almost entirely on interviews.

143. Commissioner Nadon authorized the establishment of the Security Service's own audit unit in August 1976 as part of the changes resulting from the Security Service's achieving divisional status. The unit is headed by an Inspector, who has two Staff Sergeants reporting to him. Its mandate falls into three areas: operations, administration and planning. In the first area, operations, there is a clear overlap with the Operational Audit Unit described above. For example, the staff in the Security Service unit asks all those interviewed the following two questions concerning legality:

> Are you involved in or do you know of any investigational practices which might be of questionable legality?
>
> Are you certain that these practices have been suspended?

In addition to asking these general questions, the audit unit samples files and conducts interviews on the process of identifying groups and individuals to be investigated and on the use of intrusive investigative techniques. The auditors rely heavily on the intelligence collection goals established by the planning process. Of particular concern to the auditors would be an investigation of a group which does not relate to the yearly plan, and for which there is no written authorization from Headquarters.

144. In examining an investigative technique, the audit unit when auditing a large area command might spend up to one day going through every fifth file and then following up with interviews. The function of the auditors is to identify what appear to be questionable situations and ask for a second look, often from the officer in charge of the particular head office branch. The auditors do a similar combination of file reviews and interviews concerning the use of intrusive techniques.

145. In the planning and administration areas, there is considerable overlap between the Security Service Audit work and the management audit of the Audit Branch. The major difference is that the Security Service audit is more detailed. For example, the Security Service auditors interview some 40 to 50 per cent of the members within a unit — almost double the corresponding figure for the Audit Branch. Also, the Audit Branch does only a sample of the various area commands and headquarters units. Consequently, the frequency of these audits would be less.

146. There are several positive features to the Force's approach to auditing. The subject of the audit always has an opportunity to respond to the auditors prior to their submitting a report. The auditors do no more than identify problems, and thus do not force solutions onto the unit being audited. Finally, the audit reports are designed to identify positive as well as negative points. Nonetheless, we have some serious misgivings about the current auditing system as it affects the Security Service. Our approach to auditing has three elements: first, the major responsibility for operational auditing should be with

an organization independent of the security intelligence agency; second, there should be a small investigative unit within the security intelligence agency with responsibility for handling complaints and for reviewing agency operations on a more selective, less mechanical manner than is now the case; and third, managerial auditing should be replaced by more promising approaches to organizational improvement and change. We shall enlarge on each of these elements.

147. In the next section of the Report, we will be recommending the formation of an independent review body (the Advisory Council on Security and Intelligence) with broad responsibilities for auditing and reviewing the activities of all agencies within the intelligence community, including the security intelligence agency. We shall be elaborating on the role of this agency and the reasons for establishing it. Briefly, for our purposes here, there are two fundamental reasons for our preferring the major operational auditing responsibility to rest with an outside agency. The first is independence. During the course of our inquiry, we have heard evidence about many questionable practices — some of which we believe are contrary to, or at least not provided for by the law — which were approved by the most senior levels within the Force. We have little confidence that an audit unit based within the Force would have necessarily identified these questionable practices. We have no confidence that the work of an audit unit within the Force would have resulted in the practices, if identified, necessarily being brought to the attention of the appropriate Ministers and officials. The lack of comment by any of the audit units on the Force's handling of the Prime Minister's 1969 policy statement adds weight to our concern. So does the following testimony of a former senior Security Service officer on the audit group's access to documents relating to mail opening practices:

> Q. Would there be any way that the Audit Group, which, I assume, has the continuing function, visiting various units — is there any way in which it would have access to Exhibit B-22? [a telex dated September 23, 1977, containing Headquarters instructions to Area Commands as to the permissibility of the examination of the outside of mail and forbidding the opening of mail]
>
> A. I would expect it would have access to it if it had asked to see it; but like many things in the Security Service, and again, as I think I explained yesterday, we operate on a need-to-know basis; and because of the very sensitive nature of the CATHEDRAL operation, not only in terms of its sensitivity security wise, but, quite honestly, because it is a sensitivity in terms of illegalities, I would doubt very much whether it would have been brought to the attention of the audit people, unless they had asked for it.
>
> (Vol. 7, p. 969.)

148. A second reason for preferring an outside agency to be responsible for operational auditing is that clearly many of the problems we have been investigating had very much to do with the relationship of the Force to other parts of government. An organization which is independent of the security intelligence agency, its Minister, and the other major agencies making up the

intelligence community would be in a position to monitor these relationships and point out problem areas.

149. While urging that most of the operational auditing responsibility be lodged in an independent body, we believe that the security intelligence agency should have a small investigative unit to carry out in-depth studies of operational activities which appear to involve questionable positions. This investigative unit should also be responsible, in most instances, for investigating public complaints against members of the security agency. However, the independent review body should be informed of all complaints and the agency's response to them. Also, based on evidence before this Commission of several poorly conducted R.C.M.P. internal investigations, we believe strongly that the independent review body should be empowered, in exceptional circumstances, to investigate a complaint itself.

150. As for the management audits, we believe that the benefits simply do not match the costs. Senior management's involvement in such audits is generally confined to reviewing the final report, and perhaps following up on a small number of points. Thus, fundamental issues facing the organization seldom get addressed. We also believe that most of those being audited view management audits as nuisances, and are consequently not strongly motivated to take the results seriously.

151. One positive feature, however, of managerial auditing which should not be lost, is having 'outsiders' periodically come into an organization as catalysts for change. But rather than performing the role of an expert who examines a situation and prescribes changes for senior management, the 'outsider' (either an outside consultant or a member of some internal consulting group) would have the task of helping those within the organizational unit identify their pressing problems, understand why these problems exist, and develop solutions. To be successful, such an approach has to reverse the conditions under which auditing in the management area is unsuccessful. That is, senior management has to be involved in a substantial way, committing both time and resources; there has to be a motivation to learn among those involved in the exercise; and the learning of those within the organization requires progression, a series of opportunities to explore and experiment with new concepts.

WE RECOMMEND THAT

(a) **major responsibility for auditing the operations of the security intelligence agency for legality and propriety should rest with a new independent review body. (The functions of this body will be described in a later chapter of this report.)**

(b) **the security intelligence agency should have a small investigative unit for handling complaints and for initiating in-depth studies of agency operations on a selective basis; and**

(c) **the security intelligence agency should not allocate resources for managerial auditing, but instead should experiment with other approaches to organizational change.**

(97)

G. INTERNAL SECURITY

152. As we noted in the introductory section of this chapter, a feature which distinguishes a security intelligence agency from other government organizations is the degree to which those within such an agency are preoccupied with maintaining internal security. There is good reason for this preoccupation. As one writer on intelligence organizations puts it,

> ... an insecure service is not merely useless; it is positively dangerous, because it allows a hostile agency to manipulate the penetrated organization, as the British, for example, manipulated German intelligence during World War II. MI5 turned German agents in Britain, used them to feed false information to Germany, and thereby thoroughly confused the Germans as to the probable site and nature of the invasion of Europe. The Germans would have done better with no agents in Britain at all. At the very least they would have been jumpily alert, not knowing where the blow was to land, rather than falsely confident. It might almost be said that the better a service is, the more it is trusted by those for whom it works, the greater the potential danger it represents to its own masters. It is simultaneously the first line of defense, and the weakest link. It is an instrument perfectly designed for deception; an intelligence service is as close to a nation's vitals as a vault is to a bank's. There are enough horrible examples of manipulation in the history of espionage to guarantee that intelligence services will always look first to their own defenses.[19]

153. The primacy of security explains many of the more unusual characteristics of security intelligence work — the extreme sensitivity to what becomes public about the organization, the tendency toward insularity and distrust of those outside the organization, the intrigues of doubling and redoubling enemy agents, and the clandestine meetings in 'back alleys'. Moreover, the security question lends an important psychological feature to relationships within the organization. A fundamental assumption of all security services is that they have been penetrated. To assume otherwise is to leave themselves vulnerable to a high degree of manipulation. But this assumption leads those within the agency to spend their lives suspended between doubt and trust, suspicious of everyone including their friends, and making conscious choices about whom to trust. Most people in other fields are never obliged to make such judgments about their colleagues. In the security field the necessity to make these judgments results in the development of strong bonds among colleagues.

154. The defences erected by a security intelligence agency to protect itself are of various kinds. Perhaps the most important is the compartmentalization of knowledge. Only those with a need to know should be privy to sensitive information. A second line of defence is to screen carefully new employees entering the agency and to provide some system for ensuring the continued reliability of existing employees. And third, there are security procedures for protecting the area in which the agency is housed, its information, and its

---

[19] Thomas Powers, *The Man Who Kept the Secrets*, Alfred A. Knopf, New York, 1979, p. 66.

communications. We examine each of these defence systems in turn below. We also review current Security Service procedures for conducting internal security investigations.

The 'need to know' principle

155. An employee of the Security Service has a need to know, if he requires access to particular classified material in order to carry out his duties properly. The following factors are relevant to deciding if an employee requires access:

1. Is there an absolute operational and/or administrative necessity to have access?
2. Can the person contribute to the objective or operation by virtue of his experience, rank special qualifications or attributes?
3. Can anyone else who is briefed to have access in the operation be used in order to limit the number to a minimum?
4. Is the person conversant with the security procedures devised to safeguard classified information?
5. Does he require further education on security procedures before being granted access?

156. Of the reasons cited for applying the 'need to know' principle, by far the most important is the need to minimize the damage of an unknown penetration by an enemy agent. Other reasons for applying the principle include reducing the likelihood of leaks, and lessening the danger that sensitive information may become known through carelessness.

157. Those within the Security Service made clear to us that the principle applies primarily to continuing operations and to current intelligence gained from continuing operations. It would not appear to apply so strictly to information about certain other facets of the Service — which could be generally known by members of the Service but which should not be made public.

158. The above description of the 'need to know' principle gives little hint of the difficulties in applying it and indeed, the potential abuses the principle can lead to. The evidence before us and our own research of Service files suggests that these can be substantial. Some of the more significant problems are outlined below.

— The principle assumes that files are classified correctly. Our impression, gained over the course of three years, is that Service files tend to be overclassified. The result is that the principle is not rigorously applied because many regard the Secret and Top Secret designations as not necessarily signifying highly sensitive information.

— There are difficulties in applying the principle consistently in matters affecting several departments. We had one good example of this problem in a matter affecting the R.C.M.P. and the Department of National Revenue. (Vol. 50, p. 7995.)

— The application of the principle can lead to feelings of frustration and mistrust from employees who are excluded from knowing certain information. They may feel their exclusion was based not on security reasons but on other factors, such as a deliberate attempt to reduce their influence in the agency.

— Cooperation between two organizational units may be hampered by the 'need to know' principle. Security Service members cited several examples of two units working at cross purposes because vital information was not shared between them.

— Teamwork may be curtailed because of the principle.

— The 'need to know' principle may reduce the quality of training and development within the agency. More junior members within a branch will not be aware of many sensitive operations underway, and consequently their experiential learning will not be as rapid. Similarly, certain types of instructive case material will not be available for formal training reasons.

— The quality of decisions may be lessened in certain instances because the number of people who can comment on an operation is minimized.

— The restrictions in the horizontal flow of information may mean that normal peer pressure is not brought to bear on questionable acts.

— Persons whose function it is to oversee or inspect operations may be denied complete access to the necessary information to perform this function. For example, as we noted earlier in this chapter a senior Security Service officer testified before us that, because of the 'need to know' principle, certain audit groups within the Force did not likely know about mail openings. (Vol. 7, p. 969.) The Church Committee in the United States uncovered a similar set of examples.

— The principle may be abused by some who use it as a rationale for ignoring normal control procedures. One Security Service member, for example, who was involved in the taking of dynamite, told us that he did not tell his superiors about the incident because of the 'need to know' principle. (Vol. 77, pp. 12404-5.)

159. What this list of difficulties, costs, and potential abuses suggests is that a security intelligence agency should pay a great deal of attention to how the 'need to know' principle is being applied. In our view, such is not the case in the R.C.M.P. Security Service. We have found little written about the principle and there appears to be only passing attention given to it in training courses. Moreover there does not appear to us to be sufficient sensitivity within the Service to the potential problems associated with the application of the principle. We asked the Security Service to examine the 'need to know' principle with particular emphasis on its impact on managerial functions. A key paragraph in the reply to this request was the following:

> Our review of the subject indicates that in our mind what you are raising is essentially a "non question". Managers must manage, and in doing so must adequately supervise the work of subordinates. To properly supervise, they have a right to know what the subordinate is working on, how he is proceeding and what he is gaining. "Need to Know" does not, therefore, impact on the managerial function.

160. This reply appears to us to ignore a rather delicate set of judgments which must be made constantly in the day-to-day workings of the agency. On the one hand, an overzealous application of the principle will likely result in reduced effectiveness and greater risks of questionable activities both being undertaken and going undetected. On the other hand, if the principle is taken too lightly, risks of security breaches are increased. The impression we have gained through numerous discussions with Security Service members is that over the last decade the balance has been gradually redefined within the Service to stress an increasingly less rigid application of 'need to know'. The impact of our recommendations may continue this shift by involving more people outside the agency, including Ministers and senior officials, in decisions which affect agency operations. Having said this, we believe it important that certain very sensitive agency information continue to be subject to a very strict application of the principle. In our view, Ministers and senior officials should be given this type of information only in the most exceptional circumstances.

Security screening for agency employees

161. Responsibility for the Security Service's current screening for its own employees rests with the Internal Security Branch established in 1971.

162. In addition to the Headquarters staff, there are security coordinators connected with the area commands. Their duties mirror those of their Headquarters' colleagues: security screening interviewing; conducting investigations; ensuring that adequate security standards are maintained and so on. There is a yearly conference of area representatives and their Headquarters' counterparts.

163. As with the rest of the federal government, the Security Service's procedures for screening its employees are governed by Cabinet Directive 35 (CD-35). Approved in 1963, this directive outlines the security criteria for rejecting applicants for employment in sensitive jobs and the procedures for doing so. In a subsequent chapter of this Report we shall describe CD-35 in more detail and the changes we propose to the system for screening public servants. Suffice it to say here that three principles should apply to the security intelligence agency: first, it should have a more stringent set of screening procedures for its employees than the Public Service; second, the agency should have a less stringent set of conditions for releasing an employee for security reasons; and third, the appeal process for the agency, while recognizing the differences in its screening standards, should be the same as that of the Public Service. These principles are premised on the belief that a security intelligence agency is one of the most important targets within government for hostile foreign intelligence agencies to penetrate.

164. In addition to recommending these three broad principles, we can make in this section a number of other, more specific recommendations concerning screening procedures for Canada's security intelligence agency. We begin by noting the emphasis the Security Service now places on interviewing the candidate for security clearances. Indeed, a portion of what the staff of the Internal Security Branch do is security interviewing. This is not common practice with the rest of the Public Service, and in a later chapter of this Report, we shall be recommending that it become so.

165. Despite the heavy emphasis on interviewing within the Branch, none of its employees has any special training in this area (although a course now exists for enhancing this skill), nor were they chosen for the job with this skill in mind. This is another example of the inadequacy of the heavy reliance on a generalist approach to careers within the Service. The qualities of a good interviewer — perceptiveness, sensitivity, the ability to probe without appearing offensive, a capacity for empathy — are not common to everyone, nor can they necessarily be taught. Selection for these jobs should be done with much greater care.

166. Another concern we have about current Security Service screening procedures focusses on the decision-making process for rejecting applicants for employment on security grounds. CD-35 can be interpreted to mean that refusal to hire an applicant (from outside the Public Service) on security grounds must be made by the head of the agency or the Deputy Minister. A decision to fire an existing public servant on security grounds must be made by the Governor in Council. In contrast, in the Security Service, a relatively junior officer, has the responsibility for refusing on security grounds to hire a new employee transferring from the Public Service or from within the Force. In addition, the procedure in CD-35 for dealing with a security problem related to an existing public servant is quite elaborate. Among other things, the Deputy Minister or head of agency must personally interview the employee in question. Furthermore, the employee must be "... advised to the fullest extent possible without jeopardizing important and sensitive sources of security information, why doubt continues to be felt concerning his his loyalty or reliability". In spite of the provisions of CD-35 in the case of the Security Service, it is not Force policy to disclose reasons for rejection on security grounds.

167. We believe that the Deputy Solicitor General, on the advice of the Director General, should take responsibility for refusing to grant a security clearance. Such a decision can have a great impact on an individual's life and should not be made lightly. Furthermore, the security intelligence agency should comply with the provisions of CD-35 with respect to disclosure to the employee as to the grounds for his rejection.

Other internal security procedures

168. The Security Service's approach to other aspects of internal security — protecting the area in which the Service is housed, its information and its internal communication systems — is similar to what we have documented above. That is, the Service appears to place insufficient priority on these matters and the quality of the analysis and innovative thinking which go on is rudimentary at best.

169. Complaints we have examined simply reinforce many of the recommendations we have already made in the sections on need-to-know and security screening. The security intelligence agency must assign greater importance to internal security matters; it should staff its Internal Security Branch with more senior, better qualified personnel; and it should improve its capacity for analysis in matters relating to internal security. To do otherwise is to forfeit the agency's claim of being the government's experts on security matters.

Investigating breaches of security

170. By breaches of security we mean the following: 'leaks' of security intelligence information to someone who will make the information public (media employees, or a Member of Parliament); evidence of a possible spy or spies within the security intelligence agency; and a variety of other acts resulting from carelessness on the part of agency employees, such as losing a sensitive document. Of these, leaks of agency information present some difficulties which we now examine. Some leaks from public institutions have likely been in the public interest, some, on the other hand, have been made on the basis of self-serving motives. Moreover, leaks are an unreliable method of controlling an institution like a security intelligence agency. They often involve great risk and consequently tend to be sporadic. More importantly, leaks sometimes force individuals to make difficult moral judgments, often in emotionally charged situations. In essence, those contemplating leaking information must decide themselves, often with incomplete knowledge, whether the benefits of publicizing certain information might outweigh the potential damage. Finally, a security intelligence organization with a reputation for susceptibility to leaks is likely to become less effective. It will have more difficulty recruiting informers who may fear unexpected publicity. Also, foreign agencies may become less willing to give the agency information.

171. Our approach is to encourage employees to disclose questionable activities of the security intelligence agency to the independent review body whose make-up and functions we shall cover in more detail in a later chapter. Provided with a convenient depository for such information, the individuals involved in the disclosure will not be forced to make the difficult judgment themselves about whether public disclosure is in the best interests of Canada. (How the independent review body would deal with such information will be covered in another chapter.) Moreover, we propose that no agency employee should be punished or have his career retarded for disclosing information to the independent review body. In this way, the personal risks of disclosure are lessened.

172. For those disclosures not made to the independent review body, we recommend that the security intelligence agency launch an investigation which, in cases involving very sensitive information, should include the police. As well as attempting to discover those responsible for the leaks within the agency, the investigators should seek to learn why these leaks occur. Such leaks are likely signs of something unhealthy about the agency — poor recruiting practices, employees at lower levels in the organization feeling cut off from senior management, or other ineffective management and personnel practices.

173. At this point, we should note another questionable facet of the Security Service's current approach to internal security. That is the lack of clarity concerning the role of the Internal Security Branch in investigating and resolving breaches of security. The Branch is not fully informed about nor does it not take an active role in many security investigations. Rather, responsibility for initiating such investigations lies with the operational branches. The Chairman of an R.C.M.P. task force, in the fall of 1979, recognized this same problem

and recommended that a unit be created with substantial authority and responsibility to oversee all security related matters. This unit should have the capability and responsibility of research and it should investigate all matters considered to be a threat to the security of the Security Service including penetrations, leaks and personnel misbehaviour.

174. We concur with this recommendation, and see no reason why the unit referred to by the task force should not be the Internal Security Branch, but staffed with more senior people with specialized skills. We especially like the idea that the Branch should assume a research capability.

WE RECOMMEND THAT the security intelligence agency

(a) review regularly how the 'need to know' principle is being applied within the agency and whether the balance between security on the one hand and effectiveness on the other is appropriate;

(b) ensure that the principle is being applied to primarily operational matters;

(c) ensure that the principle is not used as an excuse to prevent either an auditing group or a superior from knowing about questionable acts;

(d) improve its training programmes with regard to the rationale behind and the application of the 'need to know' principle.

(98)

WE RECOMMEND THAT screening procedures for security intelligence agency employees

(a) be more stringent than those employed for the Public Service;

(b) ensure that the Deputy Solicitor General, on the advice of the Director General, is responsible for denying a security clearance to an individual;

(c) specify that the agency has a responsibility to advise an individual who is not granted a security clearance why doubt exists concerning his reliability or loyalty so long as sensitive sources of security information are not jeopardized.

(99)

WE RECOMMEND THAT the security intelligence agency have a less stringent set of conditions than the Public Service for releasing an employee for security reasons.

(100)

WE RECOMMEND THAT the security screening appeal process for agency employees be identical to that of the Public Service, except for the application of more demanding screening standards.

(101)

WE RECOMMEND THAT the security intelligence agency's internal security branch

(a) be staffed with more senior people who have the necessary interviewing and analytical skills;

(b) develop a research and policy unit which would keep track of and analyze all security incidents of relevance to the agency;

(c) participate in or be kept fully informed of all investigations relating to security.

(102)

WE RECOMMEND THAT agency employees be encouraged to provide information about questionable activities to the independent review body (the Advisory Council on Security and Intelligence), and that any employees who do so should not be punished by the agency.

(103)

CHAPTER 3

STRUCTURE OF THE SECURITY INTELLIGENCE AGENCY: ITS LOCATION WITHIN GOVERNMENT

A. OUR APPROACH TO THE QUESTION

1. Our major recommendation in this chapter will call for a security intelligence agency which is separate from the R.C.M.P. This new agency will be markedly different from what the Security Service has been in the past. It will be more closely integrated with the rest of government. It will be civilian in character in that its members will not have the usual "peace officer" powers nor will they necessarily be recruited primarily from the national police force. Its management and personnel policies will be significantly altered so as to attract a well-educated, widely experienced staff and keep them productively occupied. As outlined in our discussion in Part V, the new agency will have a comprehensive mandate approved by Parliament. It will have responsibilities similar to those of the present Security Service, but with some important differences. For example, there will be a shift in emphasis in the work of the new agency: there will be less concentration on the writing of routine reports, more emphasis on advising government about policy matters relating to the agency's mandate, and on providing longer term 'strategic' analyses concerning security threats to Canada. In addition, the new agency will not have a mandate to disrupt domestic political groups, either through "dirty tricks" or through other measures with the same objective.

2. We have not approached this question of where the security intelligence agency should be located in government in any doctrinaire manner or with preconceived ideas. None of us had any views on this issue before commencing our work as Commissioners. Nor, during the course of our work, did we discover an overarching principle which made our decision inevitable. What, then, is our rationale for preferring a security intelligence agency outside the R.C.M.P.? Very soon after we began our work as Commissioners, it became obvious to us that, if we were to fulfill our terms of reference, we had to propose to government a *system* for Canada's security intelligence function — a system made up of several parts, including a mandate for the agency, an approach to personnel and management issues, and a set of policies and organizational structures to ensure that the agency would be directed and controlled by government. As our work progressed and as the main parts of our proposed system took on increasing clarity, the question of the location within government of the security intelligence agency came into sharper focus. In

essence, the question was: Where within government should the security intelligence agency be located so that the security intelligence system which we were proposing would best function? Our answer, based on several reasons, no one of which is necessarily predominant, is that the agency should be under the direction of the Solicitor General and his Deputy, but not within the R.C.M.P.

3. In the section which follows, therefore, we develop the case for a separate and civilian agency. Following this, we review the arguments that have been made over several decades for retaining the security intelligence function within the R.C.M.P. We isolate those factors which are potential problem areas for a separate agency and suggest ways in which these can be overcome successfully. In the final section, we advance several recommendations on how our structural recommendations might be implemented.

B. THE CASE FOR A SECURITY INTELLIGENCE ORGANIZATION OUTSIDE OF THE R.C.M.P.

4. In this Report, we are advocating a myriad of changes to the security intelligence function of government — changes which will affect every facet of the Security Service's operations. We believe that a significant number of these changes will be resisted by the R.C.M.P. if the Security Service remains within the Force. As we demonstrated in Chapter 1 of this Part, the R.C.M.P. in the past has vigorously resisted proposed changes which run counter to its deeply held traditions and beliefs. Of the changes which the R.C.M.P. will have great difficulty in accepting, there are two which we consider to be absolutely crucial if the security intelligence agency is to perform effectively in a lawful and proper manner. These are:

(a) implementing management, recruiting and other personnel policies appropriate to a security intelligence agency; and

(b) developing suitable structures and procedures to ensure that the security intelligence agency is under the direction and control of government.

Implementation of change in these two areas would result in a new philosophy emerging — a philosophy which would affect both the internal operations of the agency and its relationships with the rest of government. It would be a philosophy based on respect for the law and for other liberal democratic principles which the agency was created to secure. It would also be a philosophy based on a high regard for effectiveness in providing government with good quality advice and information about security threats to Canada. We examine the required changes in more detail below and explain why we are convinced there is a better chance to achieve them in a separate agency.

Appropriate management and personnel policies

5. In the last chapter, we recommended significant departures from current management and personnel policies governing the Security Service, including the following: the recruitment of more mature, more experienced, better-

educated personnel with a variety of backgrounds in other institutions; a new approach to career paths; a more participatory, less authoritarian style of management; and substantially different training and development approaches. What are the prospects for implementing these appropriate personnel and management practices, if the Security Service were to remain within the R.C.M.P.? We have considered several approaches. The first is changing the Security Service along the lines we are proposing, but keeping it within the Force together with the largely unaltered criminal investigation side. Attempts over the past 25 years to fashion a Security Service substantially different from the rest of the Force, documented in Chapter 1 of this Part of our Report, leave us highly skeptical about this option. The Force's failure to achieve substantial implementation of the "separate" and "civilian" programme announced by Prime Minister Trudeau in 1969 is particularly revealing. This history demonstrates the difficulties which any government would face in attempting to introduce changes which run counter to the long tradition of the R.C.M.P. It is noteworthy that the current trend of the management of the Force appears to be in the opposite direction from what we consider to be desirable. The Security Service is being integrated more closely with the rest of the R.C.M.P., and for that reason we think that attempts to create the necessary changes within the Force would face almost insurmountable hurdles.

6. Some might argue that establishing a senior implementation team of 'outsiders', perhaps directed by a Minister, would overcome any resistance within the Force to the changes we have outlined in the previous chapter. Such an implementation effort would probably help, but we doubt that much would be accomplished without the enthusiastic support of the criminal investigation side of the Force. For example, it would be difficult, if not impossible, for an implementation team to impose a change in managerial approach upon the Force's senior management, given that what is at stake is not so much a matter of organization as a change of perceptions, attitudes, and values. Without such a change, good experienced people from other parts of government would not be attracted to jobs in the Security Service, nor would secondment arrangements with other institutions be easily effected and maintained. If the implementation team should manage to effect a number of senior appointments within the Security Service, the result would likely be an intensification of the frustrations and, indeed, acrimony which now surround the relationship between the Security Service and certain units responsible for administration within the Force.

7. Let us consider a second case — one in which the senior management of the Force is enthusiastic about creating a Security Service substantially different from the rest of the Force. What are the prospects for successful implementation under this scenario? The probability is remote that two quite different organizations, one many times larger than the other, could co-exist and prosper within the R.C.M.P. The Commissioner would be constantly buffetted by pressures and complaints from members of the larger organization, and by their demands to know why certain aspects of the security intelligence agency — more rapid promotions, lateral entries from other organizations, a more youthful management team, different attitudes towards

career paths and so on — could not be introduced into the criminal investigations side of the Force. Thus, enthusiasm about dramatically changing the Security Service inevitably implies an equal willingness to change other significant portions of the Force. It is always difficult for two quite different organizations to co-exist within a single structure for any length of time. Co-existence within the R.C.M.P. of two organizations such as we have been describing is virtually impossible. Only if the senior management of the Force were strongly to support the introduction of change, not only to the Security Service but also to a significant portion of the criminal investigation side of the Force, would we think it likely that appropriate personnel and management policies could be successfully implemented. We have seen no evidence of such support. Even if there were such a commitment, the very size of the organization, and its long traditions, would make the period of change a long and painful one.

Direction and control by government

8. A key aim in the system of reforms we are proposing is to improve the relationship between the security intelligence agency and other parts of government including Parliament, the Minister responsible for the agency, his Cabinet colleagues, the Deputy Solicitor General and other senior officials in various departments and agencies concerned with security intelligence matters. In Part V of this Report, dealing with the agency's mandate, we developed a set of recommendations designed to place the agency's use of intrusive investigative techniques under closer scrutiny of the Solicitor General and senior government officials from several departments. In Part VIII, where we focus on how the security system is to be directed and reviewed, we further develop this theme of integrating the security intelligence agency more closely with the rest of government. In addition, we place great emphasis on a security intelligence agency being independent of partisan politics. The challenge for any liberal democracy is to achieve an effective security intelligence agency which is simultaneously responsive to valid government direction and review, and yet not used for partisan purposes.

9. We believe that our proposed system of governmental direction and review would work more effectively for a separate and civilian security intelligence agency than for a Security Service within the national police force. We base this belief on two reasons. First, there is an important difference in ministerial involvement required for a security intelligence agency as compared with a police force. This difference could lead to complications and abuses, should the security intelligence agency remain within the R.C.M.P. Second, the traditional, and we believe unhealthy, semi-independent relationship which the R.C.M.P. has enjoyed with government will not easily be changed. Consequently, a security intelligence agency, if it were not part of the R.C.M.P., would come under effective direction and control by government more quickly with far less difficulties. We deal with each of these reasons in turn.

10. It is clear that there are some similarities in the way in which a police force and a security intelligence agency should relate to the rest of government. These similarities are far from trivial. For example, the responsible minister

and his colleagues, in the case of both a security intelligence agency and a police force, should provide direction and guidance in at least the following areas: legislation and general policy regarding the mandate and powers of these agencies; the level of resources allocated to these agencies, and how the agencies propose to divide these resources among competing priorities (in the case of a security intelligence agency, for example, between counter-subversive, anti-terrorist and counter-espionage activities); policies and procedures concerning the use of intrusive investigative methods; the liaison arrangements which these agencies have within the Federal government, with other domestic police forces and with foreign organizations; and policies relating to internal management and personnel.

11. However, there is at least one fundamental difference in the way a police force and a security intelligence agency should relate to government. It lies in the manner in which Ministers and senior officials should be involved in decisions regarding the groups and individuals to investigate and how such investigations should proceed. In the case of a security intelligence agency, we believe that Ministers and senior officials should be actively involved in such decisions because of the ramifications these decisions can have on Canada's system of government and on its relationships with other countries. Indeed, we have proposed a formal, continually active, committee structure to deal with such decisions, and we shall make other recommendations in Part VIII on the role of Ministers. In the case of a police force, however, involvement by Ministers and senior government officials in decisions about whom to investigate and how these investigations should be conducted should be on an advisory basis only and limited to matters with significant policy implications. There are not the same political and international concerns to dictate a need for continuous governmental scrutiny. In addition, there are often more checks and balances than in security intelligence work; the courts, for instance, provide one such check, albeit an imperfect one. Moreover, the degree of secrecy is not nearly so pronounced, and this allows more scrutiny from news media sources and pressure groups.

12. In our view this fundamental difference in the relationship to government causes a potential for unnecessary complications and increasing risks of abuse if a security intelligence agency is included within a national police force. The complications may arise because of the dual role the Commissioner of the R.C.M.P. must play in dealing with Ministers and senior officials. It is not difficult to envisage situations in which it would be unclear where security intelligence interests end and police interests begin. Furthermore, Ministers and officials who deal closely with the Commissioner on security intelligence matters may find it tempting to extend this relationship into those police matters where they ought not to be intruding.

13. There is a second reason for believing that a security intelligence agency separate from the R.C.M.P. will more likely develop the relationship recommended in this Report with both the executive and legislative branches of government. The testimony before us of numerous Solicitors General, Deputy Solicitors General and Commissioners has indicated that the R.C.M.P. has had a semi-independent relationship with the Solicitor General's Department. It is

our view — and we shall be making this argument in more detail in Part X, Chapter 4 — that such a relationship should be changed. The present relationship is unhealthy for the R.C.M.P., which could benefit greatly from the added help which those outside the Force could bring in dealing with difficult problems facing the police, and it is unhealthy for the executive and legislative branches of government, which should be holding the police more accountable than is now the case. Changing the R.C.M.P.'s relationship with government will not be a simple matter. As we noted in Chapter 1 of this Part, past history suggests that the R.C.M.P. is not an organization that can be changed easily, especially in matters involving Force traditions and deeply ingrained attitudes. By separating the security intelligence agency from the R.C.M.P., we believe that the type of relationship which the agency should enjoy with government can develop more quickly with far fewer difficulties.

14. We have an additional reason for advocating a separate and civilian security intelligence agency. A police organization, especially one as large as the R.C.M.P. (it is one of the largest police forces in the western world) with responsibilities in municipal, provincial, and federal policing, is a powerful institution in a liberal democratic country. The Force's senior managers have access to sensitive information about many hundreds of thousands of Canadians. The investigative techniques for collecting this information, by their very nature, impinge on personal freedoms. Then, too, a police force makes thousands of decisions each day, — about, for example, whom to investigate, and whom to charge — which are of immense importance to the individuals concerned. When a national police force is combined with a security intelligence agency, which operates more secretly and has even more potential to damage the liberal democratic fabric of the country, it appears to us that far too powerful an organization has been created. There is a latent danger that the public will perceive such a relatively large organization, which has acquired the status of a national symbol, as part of the essence of the state. If the members of the organization come to share this perception, the myth may become reality and its members may see their authority as autonomous from and independent of Cabinet and Parliament, and thus set apart from the law. Separating the security intelligence agency from the R.C.M.P. will reduce, but not eliminate, the potential for abuse that comes with sheer size. The effect of separation will be even more significant than the reduction in numbers would imply because the Security Service presents problems of democratic control which are disproportionate to its size.

Trust in the R.C.M.P.

15. There is an important corollary to our arguments thus far for a security intelligence agency separate from the R.C.M.P. We believe that the questionable actions which we have been investigating — and these have been actions by both the Security Service and the Criminal Investigations side of the Force — have diminished significantly the trust that Canadians and their governments have in the R.C.M.P. The litany of such actions is a long one and has been discussed fully elsewhere in this Report. The events include the following. Since 1969, the Force has virtually ignored a publicly announced government

policy concerning the Security Service. It has been far too secretive about its liaison arrangements with foreign agencies. It has misled Ministers, causing them, in turn, to mislead Parliament. Perhaps most seriously, although the Force must not bear total responsibility, it tolerated, and indeed encouraged through official policy, the widespread breaking of laws. Moreover, there is evidence to suggest that senior members of the Security Service held back information from Ministers and senior officials about questionable operational practices.

16. In our opinion, the current Commissioner of the R.C.M.P. and many others in the Force are working hard to restore this trust. Nonetheless, we believe that the changes of the kind we are proposing in this Report — changes which, in particular, will dramatically alter the Security Service — are essential if the R.C.M.P. is to be restored to the high level of trust it enjoyed in the past. Some of these changes are also required on the criminal investigation side. Thus, in arguing that the R.C.M.P. will not satisfactorily implement the necessary changes affecting the security intelligence side of its operations, we are in essence saying that the Force, irrespective of the good intentions of its current senior managers, will not succeed quickly enough in regaining the requisite high level of trust to allow the new approach to security intelligence activities to get off to a satisfactory start. A fresh start is needed, one based on the establishment of a security intelligence agency separate from the R.C.M.P.

An ancillary benefit

17. An ancillary benefit of a security intelligence agency separate from the R.C.M.P. is the potential for checks and balances to develop between these organizations. One way in which those checks and balances can develop is to make one organization dependent upon the other to perform an important function. Thus, we have recommended that the security intelligence agency not have the powers of arrest, search and seizure normally granted to police personnel; and in addition, we have recommended that police personnel must accompany security intelligence personnel in surreptitious entries under judicial warrant. Before performing such actions, police personnel will need to assure themselves that the security intelligence agency is acting legally.

18. Yet another important balancing between these agencies may occur at both the policy and operational levels. Ministers and senior officials will have the experience of one investigative agency to assess requests for increased powers made by the other organization. For example, should the security intelligence agency ask the Solicitor General to press his Cabinet colleagues to widen the practice of using informers, then the Solicitor General can ask how the national police force is managing without similar powers. The interests of both organizations may sometimes coincide on these policy matters, but they need not in all cases. At the operational level the Solicitor General will have another channel of information to check the veracity of certain allegations against either the R.C.M.P. or the security intelligence organization. If one organization is involved in systematic law-breaking or improper acts, it is likely that the other organization either will know about it or at least will have heard rumours to that effect.

An invalid reason for separation

19. We believe that the case for separating the Security Service from the R.C.M.P. is a formidable one. However, there is at least one prominent, but in our view invalid, reason for a separate Security Service which has been advanced over the past 25 years. This argument can be summarized as follows. To be effective, a Security Service must perform illegal acts. A police force, because its primary function is the enforcement of laws, should not be in the position of having to break the law. Thus, the Security Service should not be part of a national police organization like the R.C.M.P. Some believe that the Royal Commission on Security in 1969 advanced this argument when it said the following:

> ... there is a clear distinction between the operational work of a Security Service and that of a police force. A Security Service will inevitably be involved in actions that may contravene the spirit if not the letter of the law, and with clandestine and other activities which may sometimes seem to infringe on individual's rights; these are not appropriate police functions.[1]

We shall leave it to others to argue whether or not the Royal Commissioners were saying in this passage that the Security Service must inevitably break the law. Indeed, we have some reason to believe that the Royal Commissioners were not aware of the ambiguity in the phraseology. Suffice it to say here that a number of people over this past decade, including a former Deputy Minister of Justice, have invoked the Royal Commission when contending for a separate Security Service (Vol. C66, pp. 9178-9200).

20. This argument is totally unacceptable, in our view, as a basis for creating a separate and civilian security intelligence agency. As we argued in an earlier chapter of this Report, there are certain principles, of which the rule of law is one, that cannot be compromised for security reasons. A security intelligence agency which does not feel itself bound to obey the law tends to destroy the liberal democratic society it was created to protect. For this reason, this argument for a separate security intelligence agency should be categorically and publicly rejected.

C. REASONS ADVANCED FOR MAINTAINING THE STATUS QUO

21. Up to this point, we have described the major benefits to be gained from separating the Security Service from the R.C.M.P. In this section we shall canvass the main arguments advanced over the last decade for keeping the Security Service within the Force. In summary form, these arguments are as follows. A separate security intelligence agency

- will be more easily penetrated;
- may become a 'political' police;
- will be less likely to act within the law;
- will provide no stimulus for 'reforming' the R.C.M.P.;

[1] *Report of the Royal Commission on Security* (1969), paragraph 57.

— will lessen, if not help destroy, the R.C.M.P.'s contribution to national unity;

— will cut the close police-security link which is the envy of other countries;

— will no longer have the advantages of belonging to a geographically dispersed R.C.M.P.;

— will result in extra financial costs;

— will have difficulties gaining the level of co-operation from the public now enjoyed by the R.C.M.P.;

— will have difficulties building up effective liaison arrangements with domestic and foreign police and security agencies;

— will have difficulties in gaining the required co-operation from the R.C.M.P.

Our objective in reviewing these arguments is to distinguish those with some substance from those which we feel to be either unsound or insignificant. In addition, we suggest how the effects of the substantive problems might be minimized. We begin by examining a number of arguments, cited by others, which we believe to be unsound.

Penetration of a separate civilian agency

22. As the reader may recall from Chapter 1 of this part of the Report, the R.C.M.P., as part of its critique of the report of the Royal Commission on Security, argued that a separate civilian agency would be more easily penetrated than a Security Service within the R.C.M.P. The Force put this argument as follows:

> It is also a fact that most western security and intelligence services have been penetrated by the Communist bloc services. The R.C.M.P. attributes the fact that the Directorate of Security and Intelligence is not penetrated (a fact that is borne out by defector sources) largely to its attachment to and recruiting from the R.C.M.P.

There are at least two problems in the way in which this argument is worded. The first is that we believe it is dangerous in the extreme for a security intelligence agency to assert that, at any given point in time, it is not penetrated. It is impossible to substantiate such an assertion. Second, and perhaps more serious, the argument as stated misleads the reader by failing to mention that the R.C.M.P.'s Directorate of Security and Intelligence has been penetrated. In the case that we examined closely, it was a regular member who became an agent of a foreign service.

23. Despite these problems, the R.C.M.P.'s argument clearly had an important impact in 1969. Thus, Senator McIlraith, who was Solicitor General at the time the Royal Commission's Report was being considered by government, testified as follows:

> Q. . . . my question is why did you not agree with the recommendation of the Royal Commission [calling for a separate and civilian security intelligence agency]?

A: We gave it very careful consideration. It would mean an impossible task in assembling in this country the number of civilians required to do the job.

It would mean a shocking risk of penetration of the [Security and Intelligence] service, and there are other reasons. . . That could be more refined perhaps, but those are the main ones — personnel and staffing and penetration.

The penetration item was very serious. In fact — well, those were my views and that was very carefully considered, and the decision taken as set out on June 26th [1969] to meet — to try to meet what seemed to be back of what was bothering the Royal Commission and at the same time cut off this awful risk of penetration and the awful difficulty of getting adequate numbers of properly trained civilian persons.

(Vol. 119, pp. 18603-18604.)

24. In the previous chapter, when we recommended the broadening of the recruiting base for the Security Service much along the lines proposed by the Royal Commission, we concluded that it had not been demonstrated that there would be a significant increase in the risk of penetration. We noted, however, in coming to this conclusion, that it is impossible to be definitive on this point one way or the other. Current evidence, including the known penetration record of the Security Service and the fact that many senior officers within the Service do not take seriously the argument that penetration risks increase with a civilian agency, suggests to us that this is an unsound argument for maintaining the status quo.

The dangers of a 'political' police

25. Some who oppose a security intelligence agency separate from the R.C.M.P. argue that such an agency will be susceptible to becoming a partisan arm of the political party in power. The result would be serious damage to our liberal democratic society. According to this view, a security intelligence organization within the R.C.M.P. will be less susceptible to this kind of abuse because of the arm's length relationship to government which police forces have traditionally enjoyed.

26. The main problem with this argument is that the solution — a police force with an arm's length relationship to government — may produce problems as serious as the partisan misuse of the security intelligence agency. As we have argued several times in this Report, the need is to have a security intelligence simultaneously under the direction and control of government, but not used for partisan purposes. Our recommendations regarding the appointment and term of office of the Director General, the role of Parliament in the governance of the security intelligence function, and the establishment of an independent review body, all have been designed to provide safeguards against partisan abuse. On the other hand, we have gone to great lengths, as witnessed by our recommendations calling for a legislative mandate and a system of controls of intrusive investigative techniques, to ensure that the security intelligence agency is effectively controlled and guided by government. We

shall have much more to say on this topic in Part VIII of our Report when we examine in more depth the roles of the legislative and executive branches in the security area.

27. The system we are proposing, in which the security intelligence agency receives guidance and direction in a non-partisan manner, is as relevant to an agency within the R.C.M.P. as it is to an agency outside the Force. It would be a grave error if the Security Service were to maintain the quasi-independent relationship with government that it has enjoyed in the past. For reasons cited earlier in this chapter, we believe that a separate and civilian agency will develop a healthier relationship with government than would a Security Service within the R.C.M.P. The spectre of a civilian agency being more susceptible to becoming a 'political' police is an invalid one, provided that this agency is operating within a carefully designed system of checks and balances.

Acting within the law

28. Another argument, the validity of which we seriously question, is that members of a security intelligence organization who have had police training and experience are more likely to act legally than those members of a civilian agency who have never been policemen. A former Solicitor General, Mr. Fox, made this argument in the following way in testimony before us.

> . . . it would seem clear to me that. . . if you do have this pool of experienced police officers who have been brought up in the tradition of a law enforcement agency, who have spent a number of years, four or five years, let us say, on the enforcement side, in specialized areas of the fight against crime in general, and organized crime in particular; and then, if you take these people and say: well, from this point on, we are offering you a career in the Security Service, and they, at that point, go through, you know, another type of briefing or training or schooling period where the main objectives of the Security Service side of the Force are brought out. . . I still think that that is the type of model, to my mind, which offers the greatest possible guarantees [of a Security Service acting within the law.]
>
> (Vol. 160, p. 24462.)

29. The evidence before us prompts our questioning the soundness of this argument. In examining the motives that led R.C.M.P. members to perform questionable acts, we heard little or no evidence that their experience and training in law enforcement acted as a brake or a check on their actions. Consider this testimony of a Security Service officer involved in the R.C.M.P.'s disruptive measures programme:

> In the period 1971-72, when the operations known as CHECKMATE were being contemplated by myself, I certainly didn't view my role in any way as a layman. I saw myself as having certain responsibilities.
>
> I saw myself as a policeman but, more particularly, I saw myself as a member of the Security Service with certain responsibilities to deal with the activities which were at that time, in our view, escalating in the country.
>
> I felt that given that set of responsibilities as long as my actions in dealing with it were responsible, were reasoned, were measured, that I was quite within propriety, if you like, to advance them without any regard to whether they were legal, lawful or unlawful.

30. Testimony of many others within the Security Service who had police training and experience leads us to three conclusions. The first is that any government would be foolish to rely heavily on those with law enforcement backgrounds as the cornerstone for ensuring that Security Service activities were within the law. In making this assertion, we are not denying the importance of proper training in the law. Rather, we are asserting that there are many other factors to consider in designing an effective system of controls for a security intelligence agency and that some of these factors may negate the benefits of legal training: for example, training and experience in law enforcement work is of little significance if the agency tolerates, or even encourages, its members to break the law in pursuit of agency goals. A second conclusion is that a civilian security intelligence organization should be able to provide its members with training in the law which is at least as good as, if not better than, that which R.C.M.P. Security Service members have received in the past. As we noted in the last chapter, training in the law for R.C.M.P. recruits at Regina accounts for only 15 per cent of their time, and, until recently, additional training in the law for Security Service members was rudimentary. Finally, we wish to state a theme we shall develop several times in this Report: training in the law for Security Service members, while useful, is no substitute for the assignment of a lawyer from the Department of Justice to the Security Service to provide legal advice and to scrutinize proposed investigations with potential legal problems. This, to us, is a more critical factor in ensuring legally acceptable behaviour and is relevant no matter where the security intelligence function is located in government.

A stimulus for 'reforming' the R.C.M.P.

31. Some argue that retaining the Security Service within the R.C.M.P. will help to stimulate other segments of the Force to initiate managerial and personnel policy reforms similar to those necessary for the Security Service. Mr. Richard French and Mr. André Béliveau, in a recent study completed for the Institute For Research on Public Policy, make this case as follows:

> There is an additional perspective which has rarely featured in discussion of the issue of civilianization versus separation. It is that the kind of broadened recruiting and more flexible staffing and promotional policies essential to the development of the Security Service are equally essential to the managerial, policy formulation, and more sophisticated investigative functions of the criminal investigation side of the R.C.M.P.... The failures of management and policy which have emerged on the criminal investigation side prohibit complacency or inertia on that side. Separation would isolate it from the model and stimulus of a civilianized Security Service.[2]

32. We have already addressed this argument earlier in this chapter and, therefore, need only summarize the main points of our discussion. It is beyond our terms of reference to comment on the main premise on which this argument is built — that portions of the criminal investigation side of the Force require the same managerial and personnel reforms as are necessary

[2] Richard French and André Béliveau, *The R.C.M.P. And The Management of National Security*, Montreal, Institute for Research on Public Policy, 1979, p. 71.

within the Security Service. Nonetheless, let us assume for the moment that this premise is valid. In this case, we believe that it is illusory to expect that the Security Service would give any significant stimulus to the rest of the Force unless the Force's senior management were deeply committed to these fundamental reforms for the R.C.M.P. as a whole or a good portion of it. The evidence of the past 25 years suggests that the Force's senior management has been steadfastly opposed to such changes. We have seen no reason to suggest that this position has changed significantly, if at all.

The National Unity question

33. A common assertion is that the R.C.M.P. contributes to the national unity objectives of the government in at least two ways.[3] First there is the Force's role as a symbol of Canada. The scarlet coated "Mountie" is familiar to every Canadian and is an integral part of this country's international image. A further contribution the Force makes to national unity, according to some, is the example it sets of an institution in which people from all parts of Canada work together for the general good, often far from their home towns or provinces. Some who advocate retention of the Security Service within the R.C.M.P. argue that there is a strong likelihood over the next decade that the R.C.M.P. role in municipal and provincial contract policing will dramatically diminish. If this were to happen, coupled with the Force's losing its security intelligence function, they contend that an important contributor to national unity would have been severely crippled.

34. For many Canadians the R.C.M.P. no doubt contributes in an important way to their sense of national identity. However, we do not believe that the R.C.M.P.'s capacity to serve as a significant Canadian symbol is dependent on the Security Service being part of the R.C.M.P. Rather, the more significant contributor in this regard is the work of the R.C.M.P. in drug investigations, and the contract policing role which results in large numbers of highly visible Mounties dispersed across eight provinces. Moreover, disclosure of improper and illegal conduct by the R.C.M.P. Security Service has probably been a negative factor in terms of national unity.

35. A second point we should make concerning this argument is this: even if the R.C.M.P. eventually loses both its security intelligence role and part or all of its contract policing role, we believe that there is still a viable and important federal policing role. Every federal democracy of which we are aware has a national police force, regardless of the country's constitutional make-up. For Canada, a federal police force would have at least the following roles: enforcing a number of federal government statutes; policing the northern territories; investigating crimes with a national or transnational dimension (e.g. organized crime, commercial crime, and crimes involving drugs) and providing certain expensive and capital-intensive police services in the fields of education, communication, and the forensic sciences. In short, the *raison d'être* of a

[3] See, for example, the Task Force on Law Enforcement's Report, *The R.C.M.P. Provincial and Municipal Contracts*, prepared by the Department of the Solicitor General, 1978, pp. 23-24.

national police force is not contract policing, nor is it in security intelligence work. Thus, there is little likelihood, no matter how future constitutional talks proceed, of Canada losing the R.C.M.P. as a national symbol.

Foreign comparisons

36. Over the past several decades, those on both sides of the question of whether the Security Service should be part of the R.C.M.P. have used foreign comparisons to bolster their case. Here, for example, is part of the R.C.M.P.'s response to the recommendation of the Royal Commission on Security for a separate and civilian security agency:

> The Commission says "*we think it probable* that association of the security function with the police role tends to make the work of the security authorities more difficult" (para. 57 of the abridged version). Just the opposite is true. The police-security link is of daily value to both sides. This is substantiated by the fact that Canada, the United States, and all the larger countries of Western Europe except the United Kingdom, Greece, and West Germany have a security service tied to a national police organization.

37. Our own research has taken us to several countries to learn about the organization and governing patterns of the security intelligence function. We have visited the United States, the United Kingdom, Australia and New Zealand. In addition, our staff have gone to the Netherlands, West Germany and France. All of these countries, except the United States, have a security intelligence organization which is not part of a national police force. The usual pattern is for the police forces to have special units to liaise with, and sometimes support, the security intelligence organization in performing its role. We found no evidence of any inclination to change the structural arrangements in these countries. Nor did we find any evidence to suggest that these arrangements had been controversial in the past. The prime exception to the above pattern is to be found in the United States. But, because there are so many agencies performing some security intelligence functions — the C.I.A., the F.B.I., the National Security Agency, the Secret Service, and three military intelligence services — exact parallels with Canada are difficult to draw. No doubt the agency with duties most closely parallelling those of the R.C.M.P. is the F.B.I. Nonetheless, the F.B.I., a national police force with no similar 'contract' policing role, is very different from the R.C.M.P.

38. Our overall conclusion from studying these foreign examples is that they do not settle the question one way or the other. Our recommendation calling for a security intelligence organization separate from the R.C.M.P. is not based on evidence we have gathered from researching security arrangements in foreign countries. But we do take comfort from the fact that variations of the solution we are proposing for Canada have proved to be practicable in other countries.

Efficiencies from a widely dispersed R.C.M.P.

39. In the R.C.M.P.'s commentary on the recommendation of the Royal Commission on Security that there be a civilian security service, the Force

argued, among other things, that "... only the R.C.M.P. is spread sufficiently widely across Canada to constitute an adequate service...". Thus, if the R.C.M.P. Security Service wished to conduct an investigation in a remote area of the country, it could, according to this contention, call on members of the local R.C.M.P. detachment already established in this remote area to conduct the investigation. The savings realized would be in reduced transportation costs and the reduction of time taken on the part of the investigator to conduct the investigation. There would also be more likelihood of detection if someone from another area were to appear suddenly in a remote community.

40. These arguments have some validity, but the actual savings involved appear to be so small as to be an insignificant factor in the decision about where to locate the security intelligence function in government. Security intelligence work is heavily oriented to the cities, and a separate security intelligence agency would understandably have personnel in all the major urban centres of Canada. Moreover, if the investigation were a sensitive one, it is likely that the Security Service personnel would do the investigation themselves, no matter how remote the area. If our recommendation is accepted that the responsibility for doing much of the routine security screening work should be shifted elsewhere in government, then there should be even less need for investigatory work in remote areas on the part of the security intelligence agency. Finally, for certain investigations, the security intelligence agency could continue to seek the co-operation of the R.C.M.P. or of the local police.

Financial costs of separation

41. A variation on the efficiency argument dealt with above is to cite the financial costs involved in actually separating the Security Service from the R.C.M.P. and creating a new agency. In our view, this argument has some merit, at least in the period immediately following the decision to re-organize. However, in the longer term, we believe that a separate and civilian agency will be more efficient from a cost point of view than a Security Service within the R.C.M.P. Let us enlarge on this argument.

42. There is no doubt that the re-organization we are proposing would, in the short run, involve extra financial costs. For example, costs would accrue in establishing the agency in accommodation separate from that of the Force. Certain services now provided to the Security Service by the rest of the Force would need to be established in the security intelligence agency, and there would not likely be an immediate and corresponding decrease in the personnel providing such services for the Force as a whole. Significant portions of the time of senior managers from several organizations including the R.C.M.P., the security intelligence agency, the Solicitor General's Department and others such as the Privy Council Office, Treasury Board, and the Public Service Commission, would be consumed in planning the establishment of a separate agency. Finally, both the R.C.M.P. and the security intelligence agency would need to establish liaison units, at least for the first few years following the structural change, and these units would increase overall costs. (We shall argue later in this chapter that these liaison units should be small.) The total of these costs would not be large, given the relatively small size of the Security Service.

For example, the senior financial officer of the Security Service has made a rough estimate that in a separate agency it would be necessary to add 100 employees to the existing Security Service staff to perform administrative and other functions now provided for the Security Service by other parts of the R.C.M.P. He estimated that for the fiscal year 1977/78, these 100 extra employees would have increased the Security Service's budget by $2.8 million. Thus, it would not be a large reorganization by Federal government standards. Moreover, these re-organization costs, over time, would decrease rapidly, in that, for example, the R.C.M.P. would be able to reduce its administrative staff.

43. The more important question, however, is what would happen to overall costs in the longer term. We believe that the security intelligence agency we are recommending, whether it is within the R.C.M.P. or separate from the Force, has the potential of performing effectively with a significantly smaller number of employees than the current Security Service. An agency separate from the R.C.M.P. will likely reduce its size more quickly and to a greater extent than would a Security Service within the R.C.M.P. Thus, the long-term prospect is that a separate security intelligence agency will be more efficient.

44. The potential for a much smaller security intelligence agency comes from several sources. For example, we are recommending that certain Security Service functions, such as much of its current efforts in investigating what we call "revolutionary subversion", not be performed at all. (As we recommended in Part V, Chapter 3, the security intelligence agency could only monitor activities falling under this category of "revolutionary subversion" but could not launch full investigations unless there were evidence of espionage, foreign interference, or serious political violence.) Another example is the reduced role in security screening. Other reductions in size can be realized by reducing current overstaffing which the senior administrative officer in the Service estimated was at least 5 per cent in late 1979. In addition, by implementing the personnel policy changes recommended by us in the last chapter, a security intelligence agency should be able to reduce its size significantly. There are many people in the current Service doing work which they do not like and are not suited for. Without a detailed survey on a unit-by-unit basis, it is difficult to make a firm estimate of just how small a new security intelligence agency could become. Several former members of the Security Service, including very senior ones, have suggested to us that a reduction in size by as much as one-third to one-half is possible and desirable.

45. A separate security intelligence agency will be able to make these reductions in size more quickly. Moreover, the reductions themselves will likely be greater. We say this for several reasons. A separate agency should result (as we shall point out later in this chapter) in an infusion of new senior managers, who will not be wedded to current Security Service programmes and who will scrutinize the existing activities of the Service more thoroughly than would the existing group of senior managers. Second, and perhaps most important, the personnel policy changes we are recommending, if they were to take place within a Security Service which is part of the R.C.M.P., would occur more

slowly than in a separate organization. Thus, fewer economies over time would be realized.

46. We should emphasize that in advancing the above arguments we are not calling for a ruthless approach in dealing with current Security Service personnel. Nor, for that matter, are we suggesting that a smaller, more efficient security intelligence agency can be realized by having the R.C.M.P. accept unwanted personnel, thus itself becoming overstaffed and less efficient. Rather, what we are suggesting is that attrition within the R.C.M.P., including the Security Service, is large enough to accommodate over several years the magnitude of personnel changes we are proposing, without a resultant overstaffing of either organization. (In the past three years members leaving the Force were as follows: 1977 — 604, 1978 — 699 and 1979 — 774.)

47. We should discuss one additional point concerning the possible effects that the creation of a separate and civilian agency will have on current Security Service staff. Some might argue that most members of the Security Service do not favour the creation of a new agency, and therefore employee morale will suffer considerably. Those making this assertion might point to the 1976 survey of Security Service members, referred to in Part VI, Chapter 1, where the members were invited to select one of four options with respect to the future of the Security Service. Of those who responded, 74% opted for choices which would retain the Security Service in the R.C.M.P. The resultant poor morale, it could also be argued, may lead, in turn, to increased costs and lowered effectiveness in the new agency.

48. We do not accept this line of argument, for the following reasons. First, it is our impression based on many informal meetings with Security Service members that a significant portion of Security Service employees would happily become members of a separate and civilian agency. Indeed, we are concerned about morale levels, especially among current civilian members, if the Security Service were to remain in the R.C.M.P. Our impression is not based on any scientific survey conducted by either this Commission or the R.C.M.P. From our discussions with members of the Security Service we believe that there is currently a much stronger desire for major structural change than the 1976 survey might, at first blush, suggest. It is important to remember that this survey was conducted prior to the revelations and attendant negative publicity for the Force that gave rise to the creation of this Commission. In addition, we have more confidence in the face-to-face format of informal meetings, where an individual's beliefs and the intensity with which these beliefs are held can be examined in some depth, than in an impersonal survey which forces a person to choose one of four options without giving him the opportunity to explain his choice or to indicate how strongly he feels about the matter. Our second reason for rejecting the argument that morale will suffer under a separate and civilian agency arises out of our conviction — and we shall be making a recommendation to this effect later in this Chapter — that no one should be pressured in any way to become a member of the new agency. Current members of the Security Service who wish to remain in the R.C.M.P. should be seconded to the new agency for a period lasting no longer than two years. Under such an arrangement, we do not believe that morale

levels within the new agency would be unduly harmed even during the transitional period when the new agency is being established.

Co-operation from the public

49. One cost of separating the Security Service from the R.C.M.P., often cited by Security Service members themselves, is that a new civilian agency would not enjoy the same degree of public goodwill as does the R.C.M.P. Here is how the authors of one recent study of the separation question, completed within the Security Service itself, put this argument:

> It is our perception that many members receive quick and extensive co-operation from the public (e.g. access to people, places, records, etc.) once they identify themselves as police officers and as members of the Force. There is considerable emotional support for the R.C.M.P. as a Canadian symbol which inclines many people to co-operate. Much of the co-operation also flows from the public perception that they have an obligation to assist the police. Any new organization concerned solely with security intelligence would take some time to establish a parallel obligation.

50. We concur with this assessment but would add the qualifier that the R.C.M.P.'s public goodwill is less of an asset in certain areas of the country — most notably in the Province of Quebec — than it is in Western Canada, where the Force's historical roots lie. How significant would be this loss of public good will if the Security Service does separate from the R.C.M.P.? In our view, the costs in terms of reduced effectiveness would not be large and would likely diminish over time. A large majority of Canadians will be sympathetic to the goals of a new security intelligence agency, especially one which is under the control of government, has a clear legislative mandate, has a significantly reduced role in investigating domestic subversion, and is prohibited from doing "dirty tricks". Over time, we see no reason why a separate civilian agency with the type of personnel we are recommending in this Report could not develop an excellent relationship with the public. Throughout our research of security arrangements in other countries, we did not find officials anywhere bemoaning the lack of public support for their civilian agencies. The targets of a security intelligence agency — foreign spies, international terrorists, and violence-prone domestic groups — do not have a large constituency of supporters in a liberal democratic country.

Liaison with domestic and foreign police and security agencies

51. In its commentary on the Report of the Royal Commission on Security in 1969, the R.C.M.P. maintained that it had "... built up meaningful liaison with security services and police forces in foreign countries which could not be readily acquired by a new service". We believe that this assessment has some merit, especially in the period immediately following the establishment of the new agency. Indeed, this assessment could be extended to include the liaison arrangements the R.C.M.P. now has with domestic police forces. Nonetheless, we believe that a new agency could quickly develop as effective a set of relationships with both foreign and domestic agencies as the R.C.M.P. now appears to enjoy. As the authors of the recent R.C.M.P. study of the separation issue, to which we referred above, noted:

It has been maintained that foreign agencies (and security units of other police forces) would be less inclined to share information and co-operate with a non-police agency. It is our view that solid relationships will quickly develop based on need. It would be incumbent on a separate Security Service to quickly develop a reputation for professionalism and to develop a product which other organizations would deem valuable.

52. Even in the period immediately following the establishment of the new agency, it would appear to us that a number of steps could be taken to reduce the liaison problems which might develop. For example, as we suggested in Part V, Chapter 8, the establishment of a special liaison unit to work with domestic police forces might help the new agency better manage these important relationships. And, following the example of its Australian counterpart, the new security intelligence agency might attempt to develop written agreements with major domestic police forces. These agreements would state how the agency and the police force would liaise with each other, and secondly, what types of assistance each could expect from the other. Perhaps the most important factor, however, in determining the efficacy of these new liaison arrangements and the speed at which they develop will be the Director General of the security intelligence agency. It is essential that he be highly competent at working with domestic police forces and foreign security intelligence agencies.

Co-operation with the R.C.M.P.

53. Of all the domestic police forces, the R.C.M.P. will be the most important in contributing to the overall effectiveness of a civilian security intelligence agency. The size of the Force, its role in municipal and provincial policing, its expertise in the forensic sciences, and the overlapping responsibilities of the two organizations in such areas as security screening, V.I.P. protection, terrorism and other forms of politically motivated violence are all factors which contribute to the importance of the security intelligence agency's relationship with the R.C.M.P. A separation of the Security Service from the R.C.M.P. will be received with hostility by some members of the R.C.M.P. and this may result in considerable initial strains in the relationship between the two bodies. Indeed, we consider a potential lack of co-operation between the Force and a separate civilian security intelligence agency as the greatest risk involved in the structural change we are proposing. It is imperative, therefore, that a number of steps be taken to minimize the possible impact of a sour relationship.

54. The Solicitor General and the Deputy Solicitor General would have a tremendously important role to play in building an effective relationship between these organizations. One of the primary reasons for our recommending that both organizations remain within the same ministry is to ensure that a Minister and his deputy place high priority on developing an adequate level of co-operation between them. The Solicitor General and his Deputy can accomplish this in several ways. They should meet regularly and simultaneously with the Director General and the Commissioner of the R.C.M.P. to review mutual problems, especially those arising from the implementation of the new structural arrangements. They can help both organizations develop a written agreement, specifying how co-ordination will be achieved. (Incidentally such an agreement might serve as a model for formalizing the relationship between the

security intelligence agency and other Canadian police forces.) They can encourage the movement of personnel between the two organizations — both through secondments and on a more permanent basis.

55. Co-ordination between the two organizations might also be enhanced, especially in the period immediately following the formation of the civilian agency, by the establishment of a liaison unit at least at the Headquarters level within each organization. Their major responsibility would be to facilitate and control the exchange of information between the two organizations. In addition, the R.C.M.P. members carrying on liaison duties should assist the security intelligence agency in any of its operations requiring personnel with police powers, but they should not have any other investigatory responsibilities relating to security. The danger here is that security intelligence officers might be tempted to ask staff within the R.C.M.P. liaison unit, whom they would know well, to launch investigations which are outside the mandate of their agency. The independent review body should be aware of this danger and monitor closely the relationship between the two liaison units.

56. Given their limited responsibilities, these liaison units need not be large. Unfortunately, comparisons with other countries do not provide a basis for a precise estimate of the number of employees required. According to a statement in the British House of Commons in 1978[4] by the Secretary of State for the Home Department, Mr. Merlyn Rees, the number of Special Branch personnel in all police forces in England and Wales numbered approximately 1,250. However, special branch work in England and Wales entails several important responsibilities — V.I.P. protection, the collection of intelligence on the activities of the Irish Republican Army, and the monitoring of people and goods passing through British ports — which engage a large portion of special branch personnel and which have no parallel for the R.C.M.P. liaison unit we are suggesting. In addition, comparisons are difficult because of the basically unitary nature of the British governmental system. In Australia, a unified federal police force has been established only recently, and thus is not helpful for our purposes. Each of two large and long established Australian State police forces — one with 9,000 employees, the other with 7,000 employees — has a small special branch. Even here, these special branches have responsibilities for V.I.P. protection, which, in the case of the R.C.M.P., are already handled by 'P' Directorate.

57. Yet another way of ensuring that the R.C.M.P. and the security intelligence agency develop close ties with one another is to make them mutually dependent. Thus, both organizations should have something to gain from co-operation. One reason, for example, for recommending that intelligence officers not have police powers is to ensure that the agency will need to rely on the police, including the R.C.M.P., to perform effectively. The R.C.M.P., on the other hand, will depend on the security intelligence agency for information on espionage offences, international terrorism and V.I.P. protection. Perhaps having the two agencies share foreign liaison personnel, especially for countries

[4] United Kingdom, Parliament, *Debates*, May 24, 1978, p. 1,718.

requiring only one person for both police and security intelligence work, is another means of ensuring co-operation.

Conclusions

58. In this section, we have reviewed the major considerations which argue against separating the Security Service from the R.C.M.P. Most of these, in our opinion, have little validity. Others, while valid, entail costs that do not outweigh the benefits of establishing a separate and civilian security intelligence agency. Moreover, we believe that steps can be taken to minimize some of these risks and problems associated with the structural change we are recommending. In the last section of this chapter, we further consider ways to implement this structural change effectively.

59. We have no illusions that removing the Security Service from the R.C.M.P. will provide an iron-clad guarantee of future behaviour which is proper, legal, and effective. Any organizational change carries with it certain risks and potential problems. In addition, it is people who put shape and form to organizational structures and breathe life into them. The organization we are recommending to carry out the security intelligence function will change over time and there is no guarantee that all of these changes will be positive. Finally, organizations are not autonomous compartments, unaffected by their environment. As the evidence before this Commission has demonstrated, a security intelligence agency is highly dependent on the system of laws and directives within which it operates and on the structures and individuals shaping its relationships with government. The agency is not likely to operate effectively, legally, and properly if other parts of this system are badly askew.

60. Having admitted that no structure can provide absolute guarantees, we should be clear that we still regard the location of the security intelligence agency within government as an extremely important issue. It is not enough to staff the agency with 'good' people. Removing the security intelligence function from the R.C.M.P. will improve significantly the prospect for creating a security intelligence system for Canada which is effective, which is under the direction and control of government, and which has a high regard for the liberal democratic principles it is securing.

61. As one way of signalling the adoption of a fresh approach to the operation and control of Canada's security intelligence function, we recommend that the separate and civilian security intelligence agency be given a new name. We propose that the agency be called the Canadian Security Intelligence Service.

WE RECOMMEND THAT the Government of Canada establish a security intelligence agency, separate from the R.C.M.P., and under the direction of the Solicitor General and the Deputy Solicitor General.

(104)

WE RECOMMEND THAT this agency be called the Canadian Security Intelligence Service.

(105)

WE RECOMMEND THAT the Solicitor General and the Deputy Solicitor General place high priority in developing ways to strengthen the relationship between the security intelligence agency and

(i) **the R.C.M.P.**

(ii) **other Canadian police forces**

(iii) **foreign security agencies.**

(106)

D. IMPLEMENTATION OF STRUCTURAL CHANGE

62. Our review of the aftermath of the Royal Commission on Security in Chapter 1 of this part of the Report suggests to us the necessity of the government developing an implementation plan if it is to get full value from our Report. One of the first questions facing the government in developing such a plan arises from our recommendation for the establishment of a separate security intelligence agency. We think that this recommendation should be dealt with as quickly as possible. Avoiding prolonged uncertainty among existing Security Service staff is one reason for urging a speedy resolution to this question. Another is that foreign liaison arrangements might suffer, should there be an extended period of confusion about what is to happen to Canada's security arrangements. While we think a failure to move quickly on this matter may cause serious damage, still we think it desirable that this decision not be made in a way which precludes the requisite parliamentary and public discussion.

63. Once the decision to form the new agency has been announced publicly, the next steps in the implementation of the new agency can proceed. We propose that the Solicitor General be the Minister responsible for directing the establishment of the new agency. To aid him in this task, the Solicitor General should appoint an interdepartmental implementation team of officials, consisting of at least the following: the Deputy Solicitor General, the Commissioner of the R.C.M.P., the head of the security intelligence agency and senior officials from the Privy Council Office, Treasury Board, Department of Justice and the Public Service Commission. This implementation team would likely require support staff.

64. Following the establishment of the new agency, the next step would be the appointment of a Director General by the Prime Minister. If arrangements to establish a separate agency were to be made by executive decision before the passage of the new Act, the new Director General would be appointed subject to his confirmation under the terms of the statute. The Director General should work closely with the Solicitor General and the implementation team to choose the senior managers for the new agency. We believe strongly that some of these senior managers should come from outside the R.C.M.P. The evidence before us suggests that a Director General, unsupported by some senior management from outside the R.C.M.P., might have difficulty in effecting quickly the type of personnel and management changes necessary to put the new agency on a sound footing.

65. With the appointment of the Director General and the senior management of the agency, the Solicitor General and his implementation team can then turn their attention to the remaining staff of the present Security Service.

As a first step, we believe that all of the Security Service's personnel, including public servants, should be assigned to the new security intelligence agency but they should retain their current status as either members of the Public Service or members of the R.C.M.P. In effect, they would be seconded to the agency for as long as two years, until either they have become full-fledged members of the new agency or they have returned to take positions in the R.C.M.P. or the Public Service. We believe that neither public servants nor members of the R.C.M.P. should be forced to become permanent members of the new agency. We also believe that, should they become members of the new agency, they should not lose financial or other benefits they currently enjoy. Furthermore, no one from the Security Service should be dismissed as a direct result of the establishment of the new agency. We do not mean by this that everyone within the Security Service will be guaranteed a permanent job with the new security intelligence agency. Rather, we are suggesting that no one should lose his or her job with the Government of Canada.

66. In addition to determining the personnel needs of the new agency and attending to the existing employees of the Security Service, those involved in the implementation of the new agency will need to focus on other matters. Some of these we have already mentioned in this chapter — for example, ensuring the viability of liaison arrangements with foreign agencies and domestic police forces. Other concerns of the Solicitor General and his implementation team will be the new physical location of the headquarters of the new agency, the orderly transfer of files, the development of appropriate personnel and management policies, and the establishment of the necessary guidelines and internal control systems which we have outlined earlier in this report.

WE RECOMMEND THAT the Cabinet make its decision quickly to separate the Security Service from the R.C.M.P.

(107)

WE RECOMMEND THAT the Solicitor General be given responsibility for implementing the establishment of the security intelligence agency. He should appoint an implementation team to assist him, consisting of at least the following: the Deputy Solicitor General, the Commissioner of the R.C.M.P., the head of the security intelligence agency and senior officials from the Privy Council Office, Treasury Board, Department of Justice, and the Public Service Commission.

(108)

WE RECOMMEND THAT the Prime Minister appoint a Director General for the security intelligence agency.

(109)

WE RECOMMEND THAT some of the senior managers for the new agency should come from outside the R.C.M.P.

(110)

WE RECOMMEND THAT

(a) existing staff of the R.C.M.P. Security Service be assigned to the new agency but continue to belong to either the Public Service or the R.C.M.P. for an interim period to be established by the Solicitor

General. No current employees of the Security Service should be forced to become permanent employees of the security intelligence agency.

(b) no current member of the R.C.M.P. Security Service lose employment with the federal government as a result of the establishment of the new security intelligence agency.

(111)

PART VII

A PLAN FOR THE FUTURE: SECURITY SCREENING

INTRODUCTION

CHAPTER 1: Security Screening for Public Service Employment

CHAPTER 2: Immigration Security Screening

CHAPTER 3: Citizenship Security Screening

INTRODUCTION

1. To diminish the risk posed by threats to Canada's security, the federal government has established security clearance programmes for immigration, for citizenship, and for positions with access to classified information in the Public Service. To a large extent security clearance decisions are based upon the information provided by the Security Service of the R.C.M.P., the investigative agency responsible for the security screening programmes. In carrying out this responsibility, the Security Service comes into contact with hundreds of thousands of Canadians. In the course of a federal Public Service field investigation, neighbours, friends, and employers may be approached. Almost all potential immigrants are interviewed by R.C.M.P. liaison officers abroad, and many are subsequently re-screened when they apply for Canadian citizenship. Because of the pervasiveness and the importance of the security screening role, we are concerned that it be carried out both fairly and effectively. We believe security screening is essential to the maintenance of the security of Canada. Having said this, we concur with former Prime Minister Pearson when he noted the importance of ensuring that "the protection of our security does not by its nature or by its conduct undermine those human rights and freedoms to which our democratic institutions are dedicated."[1]

2. Our primary concern in this part of our Report is with the role of the security intelligence agency in the security screening process. Nonetheless, to analyze this role properly, we must concern ourselves with the overall security clearance programmes for the Public Service, immigration, and citizenship. Changes in the role of the agency will have important implications for other components in these programmes. In the following chapters we discuss each of these three security clearance programmes.

---

[1] House of Commons, *Debates*, October 25, 1963, p. 4043.

CHAPTER 1

SECURITY SCREENING FOR PUBLIC SERVICE EMPLOYMENT

3. The objective of the Public Service security clearance programme is to ensure that personnel with access to secret government information can be trusted. In this chapter, we shall propose four major changes to this programme. First, we shall make recommendations aimed at reducing the number of security clearances required in the Public Service. Second, we shall propose that the security screening criteria for the Public Service be revised so as to reflect the threats to security as we have defined them in Part V, Chapter 3. Third, we believe that the role of the security intelligence agency in the security screening process should be modified to be more in keeping with the agency's mandate and the type of personnel which it should attract. Finally, we shall recommend several changes in the review and appeal process, the most important being the establishment of an advisory body to be called the Security Appeals Tribunal. This body would hear appeals and make recommendations to Cabinet on security cases involving not only the Public Service but also immigration and citizenship. Before elaborating on these proposed changes, we begin with a brief historical overview of security screening in the Federal Public Service.

A. HISTORICAL BACKGROUND

4. The need for a programme of clearance of Public Service employees was first brought to the attention of the government in 1946, when Igor Gouzenko revealed the presence of espionage activities in some of the highest and most sensitive government positions in Canada. The Taschereau-Kellock Commission, established to investigate this communication of classified information to agents of a foreign power, recommended "that consideration be given to any additional security measures which would be practical to prevent the infiltration into positions of trust under the Government of persons likely to commit acts such as those described in this Report."[2] Priority was given to this recommendation. In March 1948, a system of security screening was formalized in Cabinet Directive 4, and with it the basic pattern for security clearances was established. The R.C.M.P. was instructed to screen all employees and candidates for employment in security sensitive positions. The findings of these security investigations were reported to the individual's department where the decision to grant the security clearance would be made.

---

[2] *Royal Commission on Espionage*, 1946, p. 689.

5. At first there were no screening criteria, but the situation was soon rectified. In April 1948, Cabinet Directive 4A was passed, prohibiting members or associates of the Communist Party or Fascist organizations from employment in government positions of trust or confidentiality. In 1952, Cabinet Directive 24 introduced a distinction between 'loyalty' and 'reliability', which still pervades our screening criteria. Disloyalty involved membership in the Communist Party, or belief in "Marxism-Leninism or any other ideology which advocates the overthrow of government by force". Unreliability, from a security standpoint, referred to 'defects' of character that might lead an employee to be indiscreet, dishonest or vulnerable to blackmail.

6. Soviet Premier Khruschev's pronouncements of "peaceful coexistence" and a general easing of cold war tensions in the mid-1950s did not lead to a reduction in security screening. On the contrary, Cabinet Directive 29, issued in December 1955, was a firm restatement of the necessity for screening. Access to classified information was now established as the rationale for security screening. In addition, this Directive took the position that there could be security risks involved even when there was no access to classified information, such as anti-democratic, foreign influence in organizations controlling the mass communications media.

7. With the change in the international climate there were indications that the Soviet bloc intelligence agencies were altering their method of recruiting spies abroad. A 1955 Royal Commission Report in Australia and two U.S. Congressional Committees indicated that the Communist intelligence services were relying upon the exploitation of the vulnerabilities of individuals rather than their ideological principles. Homosexuality was a form of behaviour thought to be particularly vulnerable to blackmail. Compromise techniques followed by blackmail and attempted recruitment had been used by the Soviets against several homosexuals in the Canadian government. As a consequence of this change of tactics by the hostile intelligence agencies, the R.C.M.P.'s Security and Intelligence Directorate began a Canada-wide programme of collecting information about homosexuals.

8. As the decade of the 1950s came to an end, the security screening role of the R.C.M.P. came under public scrutiny. A series of attacks in the press and Parliament began after the suicide of the Canadian Ambassador to Egypt, Mr. Herbert Norman. It was alleged that R.C.M.P. information had been included in the material upon which the U.S. Senate Internal Security Sub-Committee based its charge that Ambassador Norman had been a Communist.[3] It was in this atmosphere of criticism that Prime Minister Pearson introduced new security clearance procedures in the early 1960s. Cabinet Directive 35 (hereinafter referred to as CD-35), issued on December 17, 1963, was aimed at reconciling the needs of security and the rights of the individual. With a few modifications this document still forms the basis for the government's personnel security clearance procedures.

---

[3] See Charles Taylor, *Six Canadian Journeys; A Canadian Pattern*, Toronto, House of Anansi Press, 1977.

9. CD-35, a confidential document until declassified in 1978 during the course of our public hearings (Ex. M-35), retained many of the features of the previous screening directives, but made several changes. One change it made was to require greater frankness in dealing with employees whose reliability or loyalty was in doubt. Further, it provided procedures for reviewing such cases both within the responsible department or agency and, if necessary, by a Board of Review composed of three of the Deputy Ministers who served on the Security Panel. In addition, more specific criteria for assessing loyalty were introduced. Confidence was not to be placed in individuals

> . . . whose loyalty to Canada and our system of government is diluted by loyalty to any Communist, Fascist or other legal or illegal political organization whose purposes are inimical to the processes of parliamentary democracy.[4]

These 'loyalty criteria' refer specifically to:

> 3. (a) a person who is a member of a communist or a fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;
>
> (b) a person who by his words or his actions shows himself to support a communist or fascist party or an organization affiliated with a communist or fascist party and having a similar nature and purpose;
>
> (c) a person who, having reasonable grounds to understand its true nature and purpose, is a member of or supports by his words or his actions an organization which has as its real objective the furtherance of communist or fascist aims and policies (commonly known as a front group);
>
> (d) a person who is a secret agent of or an informer for a foreign power, or who deliberately assists any such agent or informer;
>
> (e) a person who by his words or his actions shows himself to support any organization which publicly or privately advocates or practices the use of force to alter the form of government.

10. For the first time, specific 'character defects' considered likely to be marks of 'unreliability' were mentioned. Pursuant to paragraph 5 of CD-35, unreliable individuals were not to have

> . . . access to classified information, *unless* after careful consideration of the circumstances, including the value of their services, it is judged that the risk involved appears justified.

Included were:

> (a) a person who is unreliable, not because he is disloyal, but because of features of his character which may lead to indiscretion or dishonesty, or make him vulnerable to blackmail or coercion. Such features may be greed, debt, illicit sexual behaviour, drunkenness, drug addiction, mental imbalance, or such other aspect of character as might seriously affect his reliability;
>
> (b) a person who, through family or other close continuing relationship with persons who are persons as described in paragraphs 3(a) to (e)

---

[4] CD-35, December 18, 1963, paragraph 2.

above, is likely to be induced, either knowingly or unknowingly, to act in a manner prejudicial to the safety and interest of Canada. It is not the kind of relationship, whether by blood, marriage or friendship, which is of primary concern. It is the *degree* of and circumstances surrounding such relationship, and most particularly the degree of influence that might be exerted, which should dictate a judgement as to reliability, a judgement which must be taken with the utmost care; and

(c) a person who, though in no sense disloyal or unreliable, is bound by close ties of blood or affection to persons living within the borders of such foreign nations as may cause him to be subjected to intolerable pressures.[5]

11. Public dissatisfaction was expressed about the adequacy of the review procedures for security screening. A Royal Commission on Security was appointed in 1966, partly in response to these criticisms, and in particular to the controversy surrounding the dismissal of postal employee George Victor Spencer. The key security clearance changes recommended in the Commission's Report, published in 1969, were:

(1) *Establishment of a Security Review Board* to consider protests by public servants, or person under contract whose careers are adversely affected by denials of security clearance.[6]

(2) *Clarification of security policy with respect to separatism*: the Royal Commission stated that

"Separatism in Quebec, if it commits no illegalities and appears to seek its ends by legal and democratic means, must be regarded as a political movement, to be dealt with in a political rather than a security context. However, if there is any evidence of an intention to engage in subversive or seditious activities, or if there is any suggestion of foreign influence, it seems to us inescapable that the federal government has a clear duty to take such security measures as are necessary to protect the integrity of the federation".[7]

(3) *Changes in the role of the R.C.M.P. Security Service*: the investigative agency should provide better documented reports to the departments with comments on the validity, relevance and importance of information and a formal recommendation on whether or not to grant clearance. Field investigations should be conducted with much more tact and imagination.[8]

(4) *Extension of the scope of security screening:* security screening should be made universal for all employees in the civil service. It should no longer apply only to persons who have access to classified material.[9]

12. The Royal Commission's recommendations were only partially implemented. The Security Review Board was not established. Prior to the submis-

---

[5] *Ibid.*, paragraph 6.

[6] *Report of the Royal Commission on Security*, 1969, Recommendation 299(a).

[7] *Ibid.*, paragraph 21.

[8] *Ibid.*, paragraph 56 and Recommendation 298(d).

[9] *Ibid.*, Recommendation 298(a).

sion of the Royal Commission's report, a limited 'appeal' procedure had been established in 1967, under section 7(7) of the Financial Administration Act. This 'appeal' procedure applied only to situations where a person was dismissed from the Public Service on security grounds. In 1975 the Public Service Security Inquiry Regulations were passed pursuant to that same section. These regulations provided for the appointment of a Commissioner to hear appeals of employees dismissed from the Public Service for reasons of security. The Commissioner is empowered to make a recommendation to the Governor in Council who has final authority in the matter. Contrary to the Royal Commission's recommendations, individuals who were transferred, or failed to obtain a promotion or position, or who had had a contract terminated on security grounds, were not provided with a right of appeal. Since the enactment of these Public Service Security Inquiry Regulations, no Commissioner has been appointed because no one has been dismissed from the Public Service for security reasons. Several individuals, however, have resigned, and other cases have been resolved by the Privy Council Office in favour of the employee.

13. Contrary to the recommendation of the Royal Commission, Ministers and their officials decided to include as a security rejection criterion involvement in separatist activities of all kinds, even those which were legal and democratic. We have already chronicled, in Part V, Chapter 3, the way in which the development of this policy since 1969 impinged on the intelligence collection programme of the Security Service. Suffice it to repeat here that this dilemma was not resolved by the Cabinet decision on May 27, 1976 — a decision in force today which reads:

> The Cabinet decision of March 27, 1975 [which established the Mandate of the Security Service] was not intended to alter the policy of the government with respect to the screening of persons for appointment to sensitive positions in the Public Service, namely that:
>
> (a) information that a candidate for appointment to a sensitive position in the Public Service, or a person already in such a position, is a separatist or a supporter of the Parti Québecois, is relevant to national security and is to be brought to the attention of the appropriate authorities if it is available; and
>
> (b) the weight to be given to such information will be for consideration by such authorities, taking into account all relevant circumstances, including the sources and apparent authenticity of the information and the sensitivity of the position.

14. This decision did not resolve the practical problem of how the Security Service was to produce such information for security clearance reports, given that the Security Service was not authorized to monitor or investigate the Parti Québecois or other democratic separatist groups. The key expression "if it is available" has never been clarified by Cabinet.

15. The role of the Security Service in carrying out security screening investigations in the field has not been substantially modified since the 1969 report of the Royal Commission on Security. The civilian security service, which the Royal Commission thought would be better equipped to carry out personnel security investigations, was not created. Regular members of the

Force, supplemented by approximately eight full-time special constables, now do security investigations in the field.

16. The format of reports has changed in accordance with the Royal Commission's recommendations. The Security Service began to write more extensive reports with comments on the validity, relevance and importance of the 'adverse information' provided. Until recently the reports included recommendations as to whether or not the candidate on whom the Security Service had some 'adverse information' should be granted a security clearance. The R.C.M.P. adopted this latter practice with some reluctance. The Force at first wanted no role in the decision-making process and later wanted authorization for what it felt was a significant change in its mandate. CD-35 authorized the R.C.M.P. only to conduct investigations and report the facts:

> The functions of an investigative agency are to conduct promptly and efficiently such investigations as are requested by departments or agencies to assist them in determining the loyalty and reliability of the subject of investigation; and to inform departments and agencies of the results of their investigations in the form of factual reports in which the sources have been carefully evaluated as to the reliability of the information they have provided.[10]

As most departments found the R.C.M.P.'s advice helpful, the practice of making recommendations continued until very recently when the R.C.M.P. finally discontinued the practice, giving the lack of authorization as the reason.

17. The role of the R.C.M.P. in security screening has been misconstrued over the years. In Parliament the Security Service has been accused both of making the actual security clearance decision and of doing nothing more than supplying factual security screening reports.[11] Neither of these contentions has been a correct representation of the role of the R.C.M.P. Security Service, which has been investigating, reporting, and, until recently, recommending. The recommendations had no binding effect. The final decision as to the granting or withholding of a security clearance rested with the employing department. Nonetheless, the recommendations of the Security Service were usually given great weight by the departments and agencies.

18. Universal screening for the Public Service, recommended by the Royal Commission on Security, has not been implemented. However, a very large number of Public Service positions still require security clearance. In the ten years prior to the Royal Commission on Security, the average annual number of security screening requests was 43,700. In the years 1972-77 the average annual number was 67,602. Much of this increase can be attributed to the 35-40 per cent increase in the size of the federal Public Service and to the annual turnover of 12 per cent.

19. We now turn to a detailed examination of this security clearance programme as it has developed over the last 35 years. We examine the types of

---

[10] CD-35, paragraph 11.

[11] House of Commons, *Debates*, January 24, 1979, p. 2517.

positions requiring clearance, the criteria applied, the roles and responsibilities of the organizations involved and the review and appeal procedures in place. In each of these areas we shall make recommendations that we feel could improve both the fairness and effectiveness of the programme.

B. EXTENT OF THE SECURITY CLEARANCE PROGRAMME

20. In this section, we look at whether federal government employees, Order-in-Council appointments and Members of Parliament should require a security clearance. We also examine the issue of updating and transferring security clearances.

21. To protect government information from unauthorized disclosure, some form of screening mechanism is needed to ensure as far as possible that persons who have access to that information can be trusted. It is also necessary to ascertain the likelihood of employees attempting to subvert the institutions of government from within or influence its policies to the advantage of foreign or violence-prone organizations. However, excessive screening involves unnecessary investigations into the personal lives and political activities of individuals. In our democratic system such investigations by the state should be confined to what is clearly necessary.

Federal government employees

22. According to the authorizing document for security screening, CD-35, employees with access to three levels of classified information — Top Secret, Secret and Confidential — require screening. A 1956 handbook of the Privy Council Office entitled *Security of Information in the Public Service of Canada* describes each of these three categories. Documents are to be classified

> *TOP SECRET* when their security aspect is paramount, and when their unauthorized disclosure would cause exceptionally grave damage to the nation.
>
> *SECRET* when their unauthorized disclosure would endanger national security, cause serious injury to the interests or prestige of the nation, or would be of substantial advantage to a foreign power. (Such as: minutes of Cabinet meetings; defence matters not of vital strategic importance; current and important negotiations with foreign powers; the national budget; and scientific, technical and military developments of substantial interest to a foreign power.)
>
> *CONFIDENTIAL* when their unauthorized disclosure would be prejudicial to the interests or prestige of the nation, would cause damage to an individual, and would be of advantage to a foreign power. (Such as: personal or disciplinary administrative matters, minutes of interdepartmental meetings, political and economic reports advantageous to a foreign power, and the private views of officials.)

We have noted a tendency in the security community to overclassify documents. This tendency, which usually arises out of an abundance of caution, appears to be merely part of a general trend throughout all areas of govern-

ment. Each government department and agency is responsible for classifying its own material, and the process of classification has not been subject to careful control. Nor have uniform standards reflecting the meaning of the original classifications been applied. This tendency to overclassify has contributed to overloading the security screening programme since the number of cases requiring screening is related to the quantity of material classified. CD-35 stipulates that there should be different screening procedures for positions with access to the three classifications of information. A Top Secret level clearance requires the most extensive screening:

(1) a subversive indices check;

(2) a fingerprint criminal records check;

(3) a field investigation.

23. For 'secret' and 'confidential' level clearances a subversive indices check and a fingerprint criminal records check suffice. Although these levels do not require a field investigation, one may be requested for cause. While overclassification of all three levels of clearance is of concern to us, it is the Top Secret level clearance that is of greatest concern, since it calls for an automatic investigation into the private life of an individual. In our opinion such investigations should be prescribed only when absolutely necessary.

24. There is strong evidence to suggest that far too many investigations have been required by departments and agencies. In 1978, 67,668 requests for screening were sent to the Security Service, of which 2,405 were for Top Secret clearances requiring a field investigation. Several other factors, besides overclassification, appear to account for the large number of Top Secret clearances requested. First, the principle of CD-35, which bases screening requirements on access to classified information, has not been strictly followed. Whole areas of employment have been deemed to require Top Secret level clearance regardless of whether each and every individual has direct access to information classified Top Secret. For example, all employees of External Affairs who are eligible for postings abroad must have Top Secret clearances. Career mobility, physical proximity and ease of intra-office communications are the reasons often cited to justify these high-level clearances.

25. Second, ever since the first security clearance directive in 1948, there has been a tendency for government departments and agencies to transfer what should normally be considered personnel staffing responsibilities to the security investigative agency. Field investigations incorporate the checking of an applicant's credentials. In many instances it has become the practice to designate positions as requiring a high-level clearance where there was not even an indirect link to classified information. Two such examples are employees working with valuable government assets, such as at the Mint, or on politically sensitive programmes such as Canadian aid programmes abroad.

26. More precise and appropriate standards for identifying positions requiring security screening are needed. Assuming these standards are to remain tied to levels of document classification, then the levels of classification must be much more precisely defined and their application carefully monitored. Once

precise classification standards are established, each government department and agency must carefully identify those positions that require security screening. Similar standards should extend to government contracts.

27. The screening programme for national security purposes should be differentiated from screening for the purpose of protecting valuable government assets or politically sensitive information. In January 1979, Cabinet approved in principle a classification scheme that made such a differentiation. Interim measures have been introduced to confine security screening to positions of national security relevance. The impetus for these interim measures was Part IV of the Canadian Human Rights Act, which gives to individuals a right of access to governmental information about themselves. Under section 54(1) of the Act, security screening reports could not be exempted from access unless they are related to "national security".[12] Hence, in March 1978, the Security Service, conscious of a need to protect its information, announced that it would no longer forward screening reports unless the department or agency affirmed that the position was one requiring access to classified information. No procedure has as yet been established for assessing the reliability of persons selected for politically sensitive positions or positions with access to monetarily valuable assets. Clearly, such a system is required; however, as these positions do not require an investigation of political activities threatening Canada's security, they should not involve a security field investigation or a subversive records check. Our view in this regard is different from that taken by the Royal Commission on Security, which recommended a fingerprint and subversive records check for all employees of the Public Service, whether or not they would be likely to have access to classified material. If the occupant of the position does not require access to classified information, the position does not clearly entail a risk to security. In such cases, we feel the security intelligence agency should not be involved in the selection process.

28. Another personnel procedure that significantly adds to the number of security screenings is the practice of requesting security reports on all or a significant number of candidates for a position before the final selection. In our opinion the selection of the successful candidate should precede any request for screening. Such a procedure would reduce the number of security clearances required and would therefore be less costly and less intrusive. More important, however, if the security clearance investigation produces security relevant information about the successful candidate, he has a greater chance of having the report assessed with due consideration, rather than merely being struck from the eligible list without explanation. We will discuss this review process later in the chapter.

Order-in-Council appointments

29. Security screening for senior positions in government presents a problem. Although screening requirements are adhered to for lower-level positions in the government, they have often been ignored for Order-in-Council appointments, which include such high-level positions as heads and members of Agencies,

[12] S.C. 1976-77, ch.33.

Boards and Commissions, Deputy Ministers, Cabinet Ministers, Senators, Judges, and Parliamentary Secretaries. Pursuant to the CD-35 these appointments are subject to the same security screening requirements as other positions with access to classified information, with the one exception of Confidential level clearances where, as Prime Minister Trudeau pointed out in a memorandum for Cabinet Ministers in 1971, "it is neither feasible nor desirable that prospective appointees be required to complete the Personal History Form which is the basis of normal security clearance regulations". In such cases a check through the Security Service's records, based on the name of the appointee alone, is substituted. In practice, however, these 'Cursory Records Checks' have been used for all Order-in-Council appointments, even those who have no access to classified information. With the exception of Members of Parliament, there appears to be no justification for exempting high-level government appointees who have access to classified information from as thorough security screening as public servants. On the other hand, we do not feel that there is any justification for conducting records checks on appointments that do not entail any access to classified information or material.

30. As Mr. John Starnes stated in his evidence before us, the 'Cursory Records Check' is both ineffectual and open to abuse (Vol. 104, pp. 16418-22). Before an appointment is made, a list of names is submitted to the Security Service for a cursory check of its records; a response within a few hours will often be requested. An effective records check cannot be done under pressure of time and with no biographical data save the individual's name. Mistakes in identity can be made and unsubstantiated rumour can be reported in place of facts. The reporting of such information can have serious adverse effects on an individual's career for years. If the Security Service reports the results of a 'Cursory Records Check' verbally, there is no means of verifying later whether adverse information was ever passed on. Because of these problems, inherent in the procedure, we consider that 'Cursory Records Checks' should be discontinued for all Order-in-Council appointments, with the exception of Members of Parliament, whose situation we shall discuss below. Order-in-Council appointments are some of the most important in government; enough time should be taken to conduct a proper security check if the position entails access to classified information.

Members of Parliament and Senators

31. We have recommended that screening standards be applied consistently across government regardless of the status of the candidate. These recommendations cause us to consider whether or not the same principle should apply to Members of Parliament and Senators with access to security relevant matters. Normally Members of Parliament and Senators do not have access to classified information. The exceptions are Cabinet Ministers and Parliamentary Secretaries who have access to such information through their departmental responsibilities and their role in Cabinet decision-making. If our recommendation calling for a Joint Parliamentary Committee on Security and Intelligence is accepted, the members of that committee will also have access to security information.

32. It has been the practice to conduct 'Cursory Records Checks' on M.P.s who are being considered for appointment as Parliamentary Secretaries. Sometimes, candidates for Cabinet positions have been screened through this same procedure, but often the required Privy Councillor Oath has been considered sufficient. The appointment of a Parliamentary Secretary who is to have access to the operations of a ministry connected with national security matters and of a Senator as a Cabinet Minister requires, in practice, a full records check but no field investigation.

33. Our opinion is that there should be a modified security screening for any appointment of an M.P. or Senator to a position in which he will have access to classified information. Because of the time pressures often involved, a modified version of the present 'Cursory Records Check' will have to suffice. There is less of a danger of mistaken identity with M.P.s than other Order-in-Council appointments. The 'Cursory Records Check' is thus more acceptable in this case. Nevertheless, the present procedure needs to be modified in order both to increase its effectiveness and to avoid possible abuses. As much biographical information as possible should be given to the security intelligence agency as far in advance as is feasible. To broaden the coverage, criminal as well as security intelligence records should be checked. The Director General should personally communicate all adverse information, recorded in writing, to the Prime Minister or to the appropriate party leader in the case of a Member of Parliament who is a member of the opposition.

34. Members of Parliament should also receive a security briefing on appointment to positions involving access to security classified information. This procedure would be similar to that in effect in Britain since 1969. On the occasion of a first appointment, every British Minister is briefed by a member of the British Security Service on the threat posed by foreign intelligence agencies in their attempts to compromise or suborn those with access to classified information. The basic system of security to protect classified information is also explained to the Ministers. A report of the British Security Commission in 1973 recommended that no security screening procedure for Ministers be introduced, but that the security briefings be expanded and that the Prime Minister "should bear in mind the desirability of satisfying himself that there is no character defect or other circumstances which would mean that the appointment of that person would endanger security".[13] This information would be obtained through the Prime Minister's personal contacts, not the British Security Service.

35. Appointees to Parliamentary Committees with access to classified information should also be subjected to a cursory security screening. In these cases, however, only the members selected should be screened, not a list of potential candidates. If significant security relevant information should come to the attention of the security intelligence agency about a Member of Parliament on or about to be appointed to one of these committees, that information should be reported to the leader of the party to which the individual belongs. The

---

[13] Cmnd. 5367, 1973, p. 11.

Members appointed to these Committees should also receive a briefing by the security intelligence agency on security threats and the system established to protect public officials against such threats.

36. Any Member of Parliament who feels that his career has been adversely affected by a security report should have access to an independent review. The Security Appeals Tribunal, which we shall describe in a later section, would provide a recourse, not now available, against potential injustices.

Updating and transferability of security clearances

37. The scope of security screening involves not only the question of who should be screened but how often they should be screened. At the present time, there is a tacit understanding that security clearances will be updated through subsequent vetting every five years. While it makes sense to review an employee's security status at least every five years, it should not be necessary in most cases to recheck the files of the security intelligence agency. If sufficiently adverse information has come to the attention of the security intelligence agency since the last records check, it should already have been reported to the personnel security officer in the department. The updating of clearances should be the responsibility of this officer. An interview every five years with the employee and a check with the immediate superior would only be considered good management and an effective option to a full security vetting.

38. When a person who has been security cleared is transferred to a different department or agency, another evaluation of that person's security clearance is required. Each department and agency is responsible for its own security clearance decisions. Positions, even with the same security level of classification, might involve different levels or dimensions of security risk. The personnel security officer in the department to which the public servant has been transferred should assess the previous security screening report and interview the candidate. A transfer should not necessarily imply the need for another check of security intelligence records.

WE RECOMMEND THAT federal government positions requiring security screening be precisely identified according to clearly defined and carefully monitored standards. Top Secret clearances should be reduced to the minimum required to protect information critical to the security and defence of the nation.

(112)

WE RECOMMEND THAT the security intelligence agency not be involved in screening or selection procedures established to ensure the suitability of persons for those government positions that do not require access to information relevant to the security of Canada.

(113)

WE RECOMMEND THAT the security intelligence agency not be requested to undertake a security screening before the final selection of a candidate for a position requiring a clearance.

(114)

WE RECOMMEND THAT the Cursory Records Check for Order-in-Council appointments be discontinued. Regular security screening proce-

dures should be carried out for those appointed to positions requiring access to security related information.

(115)

WE RECOMMEND THAT

(a) there be security and criminal records checks for M.P.s and Senators who will have access to classified information;

(b) any adverse information be reported by the Director General to the leader of the party to which the M.P. or Senator belongs; and

(c) the persons appointed receive a security briefing by the security intelligence agency.

(116)

WE RECOMMEND THAT security clearances be updated every five years. This update should be the responsibility of a personnel security officer in the department. It should not normally include a security records check.

(117)

WE RECOMMEND THAT security clearances for candidates transferring between classified positions be re-evaluated by a personnel security officer in the new department. A transfer should not necessarily include a check of the security intelligence agency's records.

(118)

C. SECURITY CLEARANCE CRITERIA

39. The current security clearance criteria for Canada, found in the 1963 CD-35, reflect the concerns during the post 'cold war' era. The only additional criterion added in the past 17 years has been that of separatist affiliation or association. These security clearance criteria are in need of revision. They do not reflect current threats, nor are they consistent with the mandate proposed by us for the security intelligence agency. Rather than specify Communist, Fascist or separatist organizations, the rejection criteria should be confined to the threats defined by Parliament in the statutory mandate of the security intelligence agency. The mandate proposed by us is meant to encompass all the threats to the security of the country. Any extension in the screening criteria would place the security intelligence agency in the untenable position of being required to give information in security screening reports that it has no mandate to collect. This situation would create a very real danger that in order to fulfill its screening mandate the security intelligence agency might extend its investigatory mandate into areas otherwise prohibited. A specific consequence of this proposal to confine rejection criteria is that the May 1976 Cabinet Decision which we quoted earlier would have to be rescinded. Parti Québecois or separatist affiliation or association *per se* should not be considered a security concern. It may well be a personnel concern for such agencies as the Federal-Provincial Relations Office, but information on such political affiliation should not be requested of the security intelligence agency. Separatism may be a threat to the federal structure of Canada but, as long as legitimate political and non-violent means are employed, it is not a threat to the security of the country, using security in the sense we have used it throughout this Report.

40. Past activities or associations should not necessarily be a bar to security clearance. The granting or denial of clearance should depend upon the individual's currrent beliefs and the nature of the position for which the individual is a candidate. For example, a person who flirted with Communism as a youth should not necessarily be denied access to classified information, though it may be imprudent to hire such an individual for the first time for an extremely sensitive job that is directly related to the internal security operations of this country. We have consciously omitted past activities from the security rejection criteria we recommend below. This is not meant to imply that the security intelligence agency should stop reporting past activity and associations. Such information might well be necessary for the department to make a clearance decision. There is a difference between the criteria and the evidence needed to satisfy the criteria.

41. Besides loyalty, there is another security clearance category listed in CD-35. The so-called 'reliability criteria' are concerned with the employee's integrity, discretion and invulnerability to blackmail or coercion. There are three sources of unreliability listed in CD-35 — features of character, associations with political security risks, and family in Communist countries — yet only in the case of the second, associations with individuals listed under the loyalty criteria, does CD-35 explicitly state that it is not the fact of the association, itself, that is pertinent, but rather the circumstances surrounding that association. According to paragraph 6(b):

> It is not the kind of relationship, whether by blood, marriage or friendship, which is of primary concern. It is the *degree* of and circumstances surrounding such relationship, and most particularly the degree of influence that might be exerted, which should dictate a judgment as to reliability, a judgment which must be taken with the utmost care. . .

42. This type of qualifier should be attached to the other two criteria of 'unreliability'. Relatives and associations abroad should not necessarily be an impediment to obtaining a security clearance. Greater consideration needs to be applied in each case to ascertain the degree of influence that could be exerted upon a candidate from relations abroad, before any decision to deny clearance is made. Similarly, in order to calculate the possibility of a candidate being indiscreet, dishonest or vulnerable to blackmail or coercion, it is not sufficient merely to provide information about certain character traits such as indebtedness, drinking habits, or sexual proclivities. Rather, there must be evidence of a connection or a potential connection between these character traits and a threat to Canada's security. For instance, for a homosexual relationship or an extra marital affair to be of relevance to a security clearance decision, there must either be evidence that the candidate is having this relationship or affair with a person who is known or suspected to be a threat to Canada's security or who is somehow connected with such a threat, or alternatively, that the conduct of the candidate is such that it will make him vulnerable to blackmail.

43. Our view that character traits must be related, or potentially related, to a security threat has important implications for the type of information that a

security intelligence agency should collect about individuals. We are very concerned about the systematic collection of information on individuals solely because such individuals exhibit a certain character trait. As we noted earlier, there has been a concerted effort on the part of the Security Service for over two decades to collect information on homosexuals. This programme began as a result of reports in the mid 1950s that the Communist bloc Intelligence Services were involved in operations to recruit homosexuals with access to classified information. By the late 1950s a seven-man team was established to investigate homosexuals in sensitive government positions. In 1960 a special squad of investigators was established to interview homosexuals in Ottawa not in the government. The Security Service in several other cities was also involved in investigating homosexuals. On the basis of interviews and Morality Squad records, the Security Service had, by the 1960s, a fairly thorough knowledge of the members of the homosexual community. Because of the effectiveness of these investigations the teams of investigators were gradually reduced. Although in 1969 an amendment to the Criminal Code made a homosexual act in private between two consenting adults no longer an offence, the Security Service continued to collect intelligence on the homosexual community. The security screening branch of the Security Service became responsible for homosexual investigations. There is now one member of that branch responsible for writing security reports on homosexuals and for directing the occasional field investigation.

44. The collection programme we have described is inconsistent with the proper role of a security intelligence agency. That such a programme has not been halted years ago is a striking illustration of an insensitivity about what the Security Service ought to be securing. Moreover, it is illustrative of a poor analytical capability within the Security Service. We believe that the security intelligence agency should no longer systematically collect information on homosexuals or for that matter on any group of people solely because they exhibit a certain character trait. Such collection programmes do not conform to the principles we established in Part V, Chapter 4 for opening and maintaining files on individuals. The existing files on homosexuals that are not relevant to security ought to be destroyed.

The Profumo affair: a case study

45. The principles we have developed in this section are consistent with those enunciated by Lord Denning in 1964 in his Report on what was known as the Profumo Affair. Lord Denning considered that when the police (i.e. the police carrying out their duty to enforce the criminal law) come across discreditable incidents in the life of a Minister, they are not to report it — save only if it appears that the security of the country may be endangered. In this case, they should report the information to the British Security Service. Experience in recent years in Canada has been that the R.C.M.P. Security Service has encouraged the police, particularly in the Ottawa area, to report "discreditable incidents" to it on a much wider basis than Lord Denning's views, or our own, would regard as proper.

46. As for the British Security Service, Lord Denning said that it was a

> ... cardinal principle that their operations are to be used for one purpose, and one purpose only, the *Defence of the Realm*. They are not to be used so as to pry into any man's private conduct, or business affairs: or even into his political opinions, except in so far as they are subversive, that is, they would contemplate the overthrow of the Government by unlawful means...
>
> Most people in this country would, I am sure, whole-heartedly support this principle, for it would be intolerable to us to have anything in the nature of a Gestapo or Secret Police to snoop into all that we do, let alone into our morals.[14]

In the circumstances before him, Lord Denning found that the British Security Service had two proper roles. One was "to defend the country against any activities by or on behalf of Russian agents", and in particular those of a Russian Intelligence officer named Ivanov. The second was to consider the possibility that Ivanov might defect and help the British. Lord Denning found that the British Security Service had

> ... confined themselves to the role I have described. They had, at one critical point, carefully to consider whether they should inquire into the moral behaviour of Mr. Profumo — they suspected that he had had an illicit association with Christine Keeler — but they decided that it was not their concern. It was a new problem for them to have to consider the conduct of a Minister of the Crown, and they decided it by reference to the principles laid down for them, to wit, they must limit their inquiries to what is necessary to the Defence of the Realm: and steer clear of all political questions. And this is what they did.

Lord Denning continued:

> The only criticism that I can see of the decision is that the conduct of Mr. Profumo disclosed a character defect, which pointed to his being a security risk (e.g., the girl might try to blackmail him or bring pressure on him to disclose secret information). But at the time when the information came to their knowledge, his association with the girl had ceased. Captain Ivanov had gone. And what remained was not sufficient to warrant an infringement of the principle that the Security Service must not pry into private lives. At any rate, it was not such a risk as they should investigate without express instructions.[15]

Thus Lord Denning appeared to accept that, if Mr. Profumo's association with Christine Keeler had not ceased, the Security Service would have been justified in continuing to investigate or "pry into" Mr. Profumo's life because his "character defect" made him a security risk.

47. The recording of such information is acceptable when so obtained because it may in due course be relevant to the investigation. But when the investigation is complete, if the information about the person's private life is no longer relevant to any suspected security risk, it ought to be discarded. It is not clear from the passage quoted what Lord Denning's view would have been if a

---

[14] Cmnd. 2152, 1963, paragraph 230.

[15] *Ibid.*, paragraphs 233 and 234.

Russian Military attaché had not been connected with Mr. Profumo's affair with Christine Keeler. Where the illicit behaviour is connected with a foreign intelligence agent its security relevance is clear as is the security intelligence agency's mandate to investigate and, if the incident points to a security risk, to report it. But what if there is no discernible relationship between the personal behaviour and a subversive political activity, and the concern is simply that the Minister is involved in circumstances which make him highly vulnerable to blackmail? Should the security intelligence agency ascertain the reliability of a report of such behaviour, and if they find it reliable, report it to the Prime Minister? We believe that the agency should ascertain the reliability of such information, and if it is reliable, report it to the Prime Minister in the case of a Minister, or to the appropriate Deputy Minister in the case of a public servant in a security classified position.

WE RECOMMEND THAT a person should be denied a security clearance only if there are

(1) Reasonable grounds to believe that he is engaged in or is likely to engage in any of the following:

(a) activities directed to or in support of the commission of acts of espionage or sabotage;

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country;

(d) revolutionary subversion, meaning activities directed towards or intended ultimately to lead to the destruction or overthrow of the liberal democratic system of government;

or

(2) Reasonable grounds to believe that he is or is likely to become

(a) vulnerable to blackmail or coercion, or

(b) indiscreet or dishonest,

in such a way as to endanger the security of Canada.

(119)

WE RECOMMEND THAT the existing Security Service files on homosexuals be reviewed and those which do not fall within the guidelines for opening and maintaining files on individuals be destroyed.

(120)

D. SECURITY SCREENING ROLES AND RESPONSIBILITIES

48. The R.C.M.P. Security Service now plays a central role in the security screening process. For Top Secret clearances, the Security Service initiates

three investigatory procedures: (1) it checks its own files for relevant information on the candidate, his relations and close associates; (2) it requests the criminal investigation side of the Force to do a fingerprint check of criminal records; (3) it does a field investigation. A Secret or Confidential level clearance requires only the first two of these procedures, although a field investigation can be initiated for cause. Based on the information it collects from these investigations, the Security Service assesses the candidate from a security standpoint and, until recently, advised the Department on whether or not to issue a security clearance.

49. In this section, we shall propose that the security intelligence agency play a much less central role in the security screening process. We shall recommend the establishment of a pool of personnel security staffing officers under the direction of the Public Service Commission, the federal government's central staffing agency. This pool of security staffing officers would be responsible for initiating the necessary investigatory procedures, for actually doing the field investigations and for liaising with and advising the departmental security officers on security clearance matters. The role of the security intelligence agency would be to provide the Public Service Commission's security staffing officers with security relevant information from its files on a candidate and, in some cases, to conduct an investigation in order to update or clarify certain information on a particular candidate or a group to which the candidate belongs. In addition, the agency should become an important source of advice on both individual security clearance questions and more general matters concerning the security clearance system as a whole. We elaborate on these proposals by examining two aspects of the Security Services current role — conducting field investigations and advising on security clearance matters.

Field investigations

50. We have four reasons for recommending the establishment of a pool of security staffing officers, under the Public Service Commission, with primary responsibility for initiating security screening investigations and actually doing field investigations. First, security screening field investigations uncover information about the personal habits and activities of an individual, and rarely disclose anything of an adverse nature relevant to the security of Canada. Thus, field investigations are primarily a personnel function in a security context, not a security intelligence function. By establishing a separate group of people to perform these investigations, the government and the people of Canada can have greater confidence that the security intelligence agency with all of its intrusive investigatory powers is confining itself to gathering and storing information which is relevant to its mandate. Under this arrangement, there can be no possible excuse for a security intelligence agency to collect information on a broadly defined group of people like the homosexual community.

51. A second reason for our central recommendation in this section concerns the control mechanisms we have established for the recruitment of human sources by the security intelligence agency. We believe that the use of human sources recruited and paid by the state must be carefully controlled lest this

intrusive investigative technique seriously damage institutions vital to our democratic beliefs. As we noted in Part III, Chapter 11, the Security Service has on occasion used the security clearance programme as a pretext for the recruitment of sources on university campuses in order to circumvent existing government control procedures. By assigning the field investigation function to another agency, we believe that this type of abuse will be less likely to recur.

52. Third, it is clear to us that a small security intelligence agency will experience difficulties in properly staffing this security screening function. As we noted earlier, much of the content of the job of a field investigator has little to do with security intelligence; consequently, it will be difficult for the agency to attract into this area security intelligence officers who have the background and skills to do the work properly. For a competent and experienced security intelligence officer, security screening does not have the attractions of many other aspects of the agency's work. By placing this function in the government's central staffing agency, we believe that it will be easier to find appropriate staff. The Public Service Commission will have the whole of the federal government from which to draw candidates. Moreover, given the similarity of the screening jobs to personnel staffing work, there might be employees within the P.S.C. itself who would be interested in spending part of their careers in this function. Those who become security staffing officers should be mature individuals well versed in the variety of political ideologies relevant to Canadian society, sympathetic to the democratic principles which the security screening process is designed to protect, knowledgeable about and interested in human behaviour and the various methods used by foreign intelligence agencies to compromise people, and above all competent at interviewing a wide variety of people.

53. Finally, having another agency in addition to the security intelligence agency with experience and expertise in the security screening function will benefit government departments and agencies by providing two sources of advice to draw from in making difficult security clearance decisions. Thus, on difficult cases, it would be wise for departmental security officers to meet simultaneously with members of both the security intelligence agency and the Public Service Commission security staffing pool to ensure that the assumptions of both agencies are carefully tested. This idea of introducing countervailing pressures into the security screening procedures parallels recommendations we have made in other aspects of security intelligence decision-making in government. We shall develop this general theme more fully in Part VIII.

54. As an alternative to creating a pool of security staffing officers in the Public Service Commission, we have considered the assigning of security screening responsibilities to the departments themselves. In departments where the volume of security work is relatively small, the Departmental Security Officer is probably not the most appropriate person to conduct these security screening interviews. While competent in the carrying out of departmental security procedures, few Departmental Security Officers are highly skilled personnel interviewers. Because we think it is essential to attain a consistently high standard of security personnel interviews and verification of references across departments, a pool of personnel security staffing officers should be

established within the Public Service Commission. These personnel security staffing officers should be assigned responsibility for specific government departments and agencies. If certain departments have the expertise and resources to meet the standards of the personnel security staffing officers in the pool, then these departments, through an arrangement similar to that now maintained by the Department of National Defence, could carry out their own security screening interview programme. We believe that the Interdepartmental Committee on Security and Intelligence should be the body to decide which departments should have responsibility for their own field investigations. In making these decisions, this Committee should ensure that there is some means of co-ordinating federal government screening activities so that these activities are done consistently and competently across the government.

55. While primary responsibility for field investigations should rest with the security staffing officers in the Public Service Commission, there are occasions when the security intelligence agency should also conduct field investigations for security screening purposes. Such occasions would occur when there is a trace or a hint of a kind of political activity on the part of a candidate that would fall within the agency's mandate. It is essential that field investigations of the security staffing officers not spill over into the investigation of political activities which is under the mandate of the security intelligence agency. Thus, the security staffing officers might become suspicious either because of a remark by the candidate himself or because of a comment by one of his referees. Alternatively, the security intelligence agency might have information on its files about a candidate — information which is dated or ambiguous and which consequently requires further clarification.

56. In addition to recommending a change in the agency having primary responsibility for the field investigations, we also propose changes in how field investigations are conducted. The current field investigation is neither effective nor appropriate as a method of meeting the security requirements of the personnel clearance programme. While the philosophy of the current investigative approach may well have been reasonably sound in 1948, from a practical standpoint the procedure is no longer viable. The increased impersonalization of society in the last 30 years has made it more difficult to obtain useful information from neighbours and employers. The strength of the civil rights sentiment has led to a growing reluctance on the part of employers and educators to co-operate with the Security Service in the screening interviews. With the advent of consumer protection legislation in the early 1970s, credit bureau checks are no longer an effective way to obtain personal financial information. Concern about maintaining the confidentiality of health records has called into question the propriety of the R.C.M.P. obtaining such records to investigate the "mental stability" of candidates for a security clearance. The R.C.M.P.'s dissatisfaction with present field investigation procedures is evident in this extract from a memorandum on security screening sent by Director General Dare to the Security Advisory Committee, on October 18, 1979.

> We are satisfied that our enquiries are not producing information which is specifically relevant to the security clearance process in over 98 per cent of the routine field investigations conducted, although it may be of some

benefit in the staffing context. And we are equally satisfied that information produced in the other 2 per cent, which usually reflects adversely on the character of the candidate, can be obtained by other means.

57. We believe that one prerequisite for obtaining an adequate insight into a person's reliability is an interview with a candidate, conducted by the Public Service Commission's security screening personnel. Second, we propose that the candidate name three referees whom the security screening officer might interview in order to gain an insight into the character of the candidate. We believe that this would be an improvement over the current practice of interviewing neighbours or employers, who in many cases may scarcely know the candidate. If the Public Service Commission security screening pool does not find the list of referees provided by the candidate to be satisfactory, then it should request additional referees as is the practice for other personnel enquiries. It should also be free to interview other persons as it sees fit.

58. Both Top Secret and Secret level clearances should require an interview of the candidate by the personnel security staffing officer. During the interview, the personnel security staffing officer should explain the security aspects of the classified position to the candidate and try to elicit any hesitations he or she may have about taking on such a position. The security staffing officer should also attempt to assess aspects of the candidate's character that would make the person particularly susceptible to blackmail or indiscretion. The interview should occur after several referees have been interviewed for a security reference. This timing would give the security staffing officer an opportunity to discuss any doubts expressed by the referees.

59. Mandatory interviews with candidates for Secret level clearances would bring the requirements of a Secret level clearance close to those for a Top Secret clearance. Until now the procedure for a Secret level clearance has been the same as that for a Confidential level clearance. In the case of both these lower level clearances, because there has been no field investigation there has essentially been no check on the "reliability" of candidates, with the one exception of the homosexual records checks. Reliability is an important criterion of screening, and should be included in Secret level clearances. An interview with the candidate should help the various government departments to assess this reliability. Interviews with the referees should not be necessary for the Secret or Confidential levels of clearance.

60. This proposed change in the security screening procedure should meet any international screening commitments Canada may have.

61. We make one final comment on the field investigation procedures. Many aspects of the current field investigation are actually personnel staffing functions. It is good employment practice to check a candidate's credentials. Academic records and employment histories, now checked as part of a field investigation, should become the responsibility of the personnel staff of the various employing departments and agencies. Credit bureau checks can equally well be carried out, if departments so desire, by personnel staffing officers.

Advisory role

62. We have already noted that the security intelligence agency should provide advice to both departments and Public Service security staffing personnel on security clearance cases, particularly those which call for careful judgments. In performing this role, the agency may find it necessary, on occasion, to clarify ambiguous or contradictory information or to update its assessment of the activities of a particular individual or group. Such is the current arrangement between the Security Service and the Department of National Defence, and it is similar to what we understand is the role of the Security Service in Britain.[16] Security intelligence officers should also provide assistance to the Public Service Commission on request by assessing information the security staffing officers have collected through interviews with candidates and their referees. If there is a difference of opinion between the security intelligence agency and the security staffing officer as to whether or not a security clearance should be granted to a particular candidate, the Departmental Security Officer should ensure that the Deputy Minister is informed of this difference.

63. In addition to advising on particular cases, the security intelligence agency should develop a competent research capacity for the purpose of providing advice to government on a variety of general matters affecting the security clearance programme including the following:

- information on the latest techniques used by foreign intelligence officers to compromise people;
- the risks posed by individuals with certain character traits;
- developments relating to security screening in other countries;
- advice on policy changes to improve the government's screening procedures.

The Security Service provides some advice in these matters but not to the extent which we believe necessary. Given its relationships with foreign agencies, and given its experience in investigating foreign intelligence officers in this country, the security intelligence agency is the organization in government best suited to provide such advice.

Criminal records checks

64. To complete this portion of our review of the security screening process, we turn to one final topic — the role of the R.C.M.P. in conducting a criminal records check. A check of records of indictable offences (using fingerprints) is part of the screening procedure for all full-time positions requiring a security clearance. This requirement, explicit in CD-35, does not apply to contract employees. Nevertheless, following the recommendation of the Royal Commission on Security that this fingerprint procedure be instituted for all those with access to classified information, a practice has developed of requesting fingerprints from some contract personnel. Fingerprinting is usually requested for

[16] See Cmnd. 1681, 1962, paragraph 70.

support staff and maintenance personnel on defence contracts, though not for professional contract personnel such as lawyers and professors.

65. The fingerprint check is inadequate as a procedure to help establish the trustworthiness of an individual about to be granted access to classified information. Only indictable offences and the 'wanted list' are checked. Summary offences, commercial fraud involvement or underworld or drug culture connections will not necessarily be uncovered by the fingerprint check. Intelligence on these other forms of criminal activity is collected in various other files in the criminal investigative side of the R.C.M.P. To obtain a more thorough verification of the absence of criminal activity these files should also be checked. If a copy of the Personal History Form is necessary to check these files, then such a form should be forwarded to the criminal investigation side of the R.C.M.P.

66. Pardoned or vacated records should be respected in security screening and should not be mentioned in security screening reports. The position we take in this regard is contrary to that of the Royal Commission on Security, which recommended that full criminal records should be available for security clearances, regardless of decisions on vacating records in other contexts. A pardon under the Criminal Records Act is granted when individuals, after a conviction, have subsequently shown that they are responsible citizens and have reintegrated into society. According to the National Parole Board the purpose of such a pardon is "to remove the stigma that so often restricts or adversely affects an individual's peace of mind, social endeavours, or career".[17] To use such a record for security clearance purposes would seem to contradict the intent of the pardon procedure.

A summary

67. At this point, it would be useful to illustrate how our proposed screening system would function. Assume that a competition has been held for a position in the Public Service with access to Top Secret information. The winner of this competition (but not the other candidates), assuming that he was not already in a security classified position, would then undergo security screening. He would fill out a personal history form and submit it along with the names of three referees to the Departmental Security Officer, who, in turn, would forward this information to the appropriate security staffing officer in the Public Service Commission. This security staffing officer would request both the R.C.M.P. and the security intelligence agency to do a records check on the candidate. If the security intelligence agency had some indication in its records of involvement by the candidate, his relations or close associates in activity which fell within its mandate, or there were some ambiguity about its information, the agency might conduct an investigation to clarify or update its records. Having received replies from the R.C.M.P. and the security intelligence agency on their records checks, the security staffing officer would interview each of the three referees. (If the staffing officer believed that any of these referees was unsatisfactory, he would request additional names from the

[17] National Parole Board, *Pardon under the Criminal Records Act*, Ottawa, 1980, p.1.

candidate. He could also interview other persons as he saw fit except to seek medical information.) Once these interviews were completed, he would then interview the candidate himself, and, if appropriate, he would review with the candidate any information that he had so far received. Given that the Deputy Minister of a department is responsible for deciding whether or not to grant a security clearance, the screening officer would summarize all security relevant information which had come to light during the screening process and, in addition, the officer would make a recommendation on whether or not to grant a clearance. In difficult cases, the security staffing officer would consult with the security intelligence agency (and possibly the R.C.M.P.) before making his recommendation to the department. In his report, he would indicate the recommendation of the security intelligence agency on the matter. This information would be sent to the Departmental Security Officer who would brief his Deputy Minister on difficult cases. The Deputy Minister, before making his decision on such cases, would likely meet with the Public Service Commission screening officer and the appropriate person from the security intelligence agency. Should the Deputy Minister decide not to grant a clearance at this point, then the review and appeal process would begin. This process is the subject of the next section of this chapter.

WE RECOMMEND THAT the federal government establish a pool of security staffing officers under the direction of the Public Service Commission with responsibility for:

(a) carrying out security screening procedures on behalf of federal government departments and agencies;

(b) conducting field investigations for security screening purposes;

(c) assessing the information resulting from the various investigatory procedures related to security screening;

(d) providing departments and agencies with advice on whether or not to grant security clearances.

(121)

WE RECOMMEND THAT Public Service Commission security staffing officers be mature individuals

(a) well versed in the variety of political ideologies relevant to Canadian society;

(b) sympathetic to the democratic principles which the security screening process is designed to protect;

(c) knowledgeable about and interested in human behaviour and the various methods used by foreign intelligence agencies to compromise people;

(d) competent at interviewing a wide variety of people.

(122)

WE RECOMMEND THAT the Interdepartmental Committee on Security and Intelligence decide what departments or agencies should have responsibility for conducting their own security screening interviews and field investigations.

(123)

WE RECOMMEND THAT the following changes be made to the field investigation procedures:

(a) for Top Secret level clearances, the Public Service Commission security staffing officers should interview three referees named by the candidate. If the list of referees provided by the candidate is not satisfactory, then the Public Service Commission should request additional referees. The security staffing officers should also interview other persons as they see fit, except to seek medical information;

(b) for Top Secret and Secret level clearances, the Public Service Commission security staffing officers should interview the candidate;

(c) good employment practices, such as checking a candidate's credentials, academic records, and employment histories should not be the responsibility of security staffing officers;

(d) in those departments and agencies which are responsible for conducting their own security screening interviews and field investigations, the functions mentioned in (a) and (b) above would be performed by their own security staffing officers.

(124)

WE RECOMMEND THAT the security intelligence agency have responsibility for:

(a) providing the Public Service Commission and departmental security staffing officers with security relevant information from its files about a candidate, his relations and close associates;

(b) conducting an investigation when necessary to clarify information or to update its assessment of a particular candidate or group relevant to the candidate's activities;

(c) advising the Public Service Commission and the employing department or agency through the security staffing officer on whether or not a candidate should be granted a security clearance;

(d) advising the federal government on general matters affecting the security clearance programme.

(125)

WE RECOMMEND THAT the R.C.M.P., as part of the security screening procedures in future, conduct

(a) a fingerprint records check and,

(b) a check of its various criminal intelligence records

for all persons with access to classified information.

(126)

WE RECOMMEND THAT pardoned or vacated criminal records not be included in screening reports.

(127)

E. REVIEW AND APPEAL PROCEDURES

68. The purpose of security screening is to ensure as far as possible the protection of information the disclosure of which might endanger the security

of the country. Nevertheless, the screening procedure must be sensitive to the requirements of individual justice and fair treatment, requirements which are essential to the very nature of the democratic system we are trying to protect. CD-35 attempted to reconcile screening procedures for the preservation of security with a review procedure that would protect the individual's rights and interests. It has not been wholly successful. We begin this section by examining some of the principal weaknesses of the review and appeal procedures contained in CD-35. We then describe the nature of the changes necessary to correct these weaknesses. Our major recommendation calls for the establishment of a Security Appeals Tribunal, an advisory body to hear appeals in the areas of public service employment, citizenship and immigration.

Weaknesses of CD-35

69. CD-35 was a classified document until it was made public by us in 1978. Previously, persons whose careers and livelihoods were adversely affected usually had no idea of the opportunities available under CD-35 to resolve doubts as to their suitability for a position requiring a security clearance. Often they would not even be told of their ineligibility for a position because they had been denied a security clearance. As a first principle, therefore, the government should publicize widely any future review and appeal procedures established for security screening purposes. In addition, the Interdepartmental Committee on Security and Intelligence should establish monitoring and control mechanisms to ensure that departments follow the review and appeal procedures.

70. Another problem with the review procedures of CD-35 is that they are not comprehensive enough. The contract employee has no right of review. Nor does the applicant from outside the Public Service. The Departmental Security Officer may request a further specific investigation to resolve the doubts raised over granting the clearance but there is no requirement to do so. Nor is there even a requirement to inform an applicant of the reason he was refused the job. The review procedures offer more protection for the individual who is already an employee of the Public Service, but even here the protection is far from complete, as the Ronda Lee case, which we summarize later in this section, illustrates.

71. Perhaps the most important weakness of CD-35, however, is the lack of an effective and independent appeal mechanism, although it does provide for some review procedures within the executive branch. According to CD-35, if doubt has been raised about the advisability of allowing an employee access to classified information and if the doubt cannot be resolved, or if further investigation is inexpedient, the assistance of the employee should be sought in an attempt to resolve the doubt. A senior officer of the department, after consultation with the Security Service, shall

> interview the subject and inform him, to the fullest extent that is possible without jeopardizing important and sensitive sources of security information, the reasons for doubt, and shall give the employee an opportunity to resolve it to the satisfaction of the responsible department or agency.[18]

[18] CD-35, paragraph 15.

Should the doubt remain, the department or agency is to withhold clearance and consult with the Privy Council Office for assistance in determining whether the employee can be informed of the situation and transferred to a less sensitive position, or whether the employee should be asked to resign, and, if he refuses, be dismissed. Before dismissal is recommended to the Governor in Council, two conditions must be met:

(a) the Deputy Minister or head of agency personally has to make a complete review of the case, including interviewing the employee;

(b) the employee must be as fully informed as possible about the charges, and allowed an opportunity to submit any information or considerations he thinks ought to be taken into account.[19]

72. There are some admirable features about these review procedures but the lack of an independent appeal mechanism is a glaring weakness. To some extent, the government has moved to correct this weakness. In 1975 the Public Service Security Inquiry Regulations were adopted. According to these regulations, if the Deputy Minister has proposed that a person be dismissed from the Public Service for reasons of security, a Commissioner may be appointed. This Commissioner has access to all files that he considers pertinent to the inquiry. The Commissioner notifies the employee that he is about to be dismissed and discloses the circumstances and information necessary to acquaint the appellant with the nature of the charges, keeping in mind the constraints of security. At the inquiry, the appellant, who may be represented by counsel, has a chance to present further evidence, including calling witnesses. Upon conclusion of the inquiry the Commissioner submits a report to the Governor in Council. It is only by a decision of the Governor in Council that an employee can be dismissed from the Public Service on security grounds.

73. As we noted in section A of this chapter, no Commissioner has ever been appointed. Since the enactment of the Public Service Security Inquiry Regulations, no one has been dismissed from the Public Service for security reasons, although some have resigned and others have been transferred or have had their careers adversely affected. Many have been denied employment or contract work. The last years for which figures are available, 1972 and 1973, indicate that for these two years 103 were denied employment for various reasons related but not necessarily confirmed as security factors, 6 resigned, and 160 were denied access, of whom 66 were transferred.

74. A recent case before the Federal Court of Appeal, that of Ronda Lee, a public servant seeking a transfer into a position requiring a security clearance, illustrates many of the shortcomings of the current review and appeal procedures for those persons whose careers have been, or are suspected of having been, adversely affected by security procedures. Ms. Lee, the successful applicant in an internal government competition for a position with the R.C.M.P., was passed over in favour of another candidate because she received an adverse security report. No attempt was made to resolve the doubts raised about her. Ms. Lee appealed the decision to the Public Service Commission Appeal Board, which determines if the merit principle has been applied in the

[19] Paraphrased from CD-35, paragraph 17.

selection of successful applicants. The Board ruled that it had jurisdiction to hear the case on the grounds that security clearance, a required qualification for the position, was a merit consideration. The Board allowed the appeal because the R.C.M.P., as the hiring department, refused to disclose the security information or the reasons for the decision to deny clearance. The Attorney General of Canada appealed successfully to the Federal Court of Appeal which held that the Public Service Commission Appeal Board had no jurisdiction to inquire into the security clearance question.[20] In an *obiter dictum*, Mr. Justice Heald noted, however, that the fact that Ronda Lee had not been afforded the opportunity, provided for in CD-35, to resolve the doubt was a "disturbing" aspect of the case, possibly forming the basis for "relief to be sought elsewhere".

Required changes

75. The case of Ronda Lee illustrates the need for improvements in the procedures for reviewing security clearance decisions. The first step is to improve the review procedures for handling adverse security reports within the executive branch of government. We believe that senior officials should make a significant effort to remove doubt about adverse security information and to ascertain if some amicable settlement is not possible. The Interdepartmental Committee on Security and Intelligence should prepare for the approval of the Cabinet Committee on Security and Intelligence a set of internal review procedures which would satisfy the following four points:

(a) The procedures must be comprehensive. They must provide for all individuals, whether public servants or not, who have been, or who suspect that they have been, adversely affected by the security clearance process.

(b) Decisions which adversely affect individuals for security reasons — these could be decisions to fire a public servant, to deny promotion or transfer to a classified position or to refuse to hire an individual — should be made by the Deputy Minister of the department concerned about the security problem.

(c) Before making such a decision, the Deputy Minister must provide the individual in question an opportunity to resolve the reasons for doubt.

(d) Before making his decision, the Deputy Minister should consult officials in at least the Privy Council Office's Security Secretariat to seek their advice on how the case should be handled.

76. When all administrative efforts to resolve the situation amicably have failed, the next step towards a more just security clearance procedure is the need to establish an appeal mechanism. The Royal Commission on Security recommended such a body, but despite public avowals of support for the idea from both government and opposition critics, the recommendation has been

---

[20] The reasons for judgment are now reported: *Re Lee* (1980) 31 N.R. 136 (Fed. C.A.). The case is now under appeal to the Supreme Court of Canada.

only partially implemented. Dismissals from the Public Service for security reasons and deportation orders against permanent residents on security or criminal grounds are the only situations where an appeal mechanism has been established. The establishment of a comprehensive security appeal procedures is a pressing issue which has not been resolved. Prime Minister Trudeau noted in the House of Commons on June 26, 1969, that the government duty to ensure the security of the State, "perhaps more than any other, requires public assurance that the measures taken in its discharge are not of a character which could infringe the basic rights of individuals or be damaging to their careers and reputations".[21] He continued:

> For this reason, Mr. Speaker, the government, after careful consideration, has decided to accept the commissioners' recommendation for the establishment of a Security Review Board. Full details of the scope, character and operation of the board are still under consideration and these may differ in some respects from the commission's recommendations...
>
> It is their opinion that such a system of review might be required in the three areas of employment, immigration and citizenship. The three basic principles which they would apply are: first, that the individuals concerned be given as many details as possible of the factors which have entered into the decisions; second, that the decisions of the Review Board could only be advisory; and third, that the importance of expertise and understanding in security matters is such that the same board should review contentious decisions in all of the three areas.
>
> With these basic principles the government agrees.[22]

77. We agree with these three principles for a security review board. We would add a fourth principle. The review body should be composed of individuals who are independent of the federal government in the sense that they are not employed by a federal department or agency. We propose that a Security Appeals Tribunal be established by statute to hear security appeals in the three areas of Public Service employment, immigration, and citizenship. In the following chapters we shall discuss in detail the appeal procedure for immigration and citizenship. In the case of Public Service positions, an independent review should be afforded all persons who have been, or who suspect that they have been, adversely affected by federal government security screening procedures, including Order-in-Council appointees, and Members of Parliament. The Security Appeals Tribunal should replace and extend the function of the Commissioner provided for in the Public Service Security Inquiry Regulations. A Commissioner of the Public Service Commission has stated publicly that the number of adverse security reports is small, "but the problem is that the number of public servants who feel their careers have been adversely affected is large".[23] We are also aware of a number of M.P.s who believe their careers have been adversely affected by unjustified or erroneous security reports.

---

[21] *House of Commons, Debates*, June 26, 1969, p. 10637.

[22] Idid.

[23] *Ottawa Citizen*, June 12, 1980.

78. The Security Appeals Tribunal must disclose to the appellant as much information as is possible without jeopardizing the security of Canada. One of the principles of natural justice dictates that the accused know all the facts of the allegations. However, insistence upon full application of this principle could seriously harm the security of Canada through the disclosure of such vital information as the identity of sources. The best compromise we can suggest is that, in order to afford the appellant reasonable reassurance that the information which he is prevented from seeing has been classified on sound grounds, the information should be reviewable by an independent Tribunal. As is provided in the Public Service Inquiry Regulations and the Immigration Act, the Tribunal must have the discretionary power to decide what information it can disclose, although it should first consult the security intelligence agency or the personnel security staffing officer as to why the information has so far been denied to the appellant.

79. The composition and procedures of this Security Appeals Tribunal should reflect the independent nature of the review. The Tribunal should consist of five members, of whom any three could compose a panel to hear appeals. The chairman should be a Judge of the Federal Court of Canada. The other members of the Tribunal should be appointed by the Governor in Council but should not be currently employed by a government department or agency. The members of the recently established Australian Security Appeals Tribunal are of similar independent calibre. The first president of the Tribunal, which reviews public service, immigration and citizenship adverse security reports, is a judge of the New South Wales Court of Appeal; the second member is a former chairman of the Australian Institute of Political Science, and the remaining members, who may be involved depending upon the case being heard, are a former Deputy Attorney General (as we would call him), a retired Air Vice Marshal and a senior academic who is chairman of a "Migrant Resources Centre."[24]

80. As in the case of appeals against dismissal from the Public Service or for deportation on security grounds, the Security Appeals Tribunal must have access to all information pertinent to the case. It should be able to require any person, other than the appellant, to supply relevant information and testimony. The appellant should have the opportunity to give evidence, call witnesses and be represented by counsel. The Australian Security Appeals Tribunal permits the Australian Security Intelligence Organization a similar opportunity to give evidence, although neither party may be present when the other is making his or her case. This procedure could be added to the Canadian security appeals process.

81. The Security Appeals Tribunal, as we envisage it, would be only an advisory body. The final decision on cases appealed to the Security Appeals Tribunal should rest with the Governor in Council. At the conclusion of its hearing the Tribunal should submit a written report and recommendation to the Governor in Council.

---

[24] *Canberra Times*, June 7, 1980.

82. It is very important that members of the Tribunal build up an expertise in security screening matters. This is a major reason for recommending that the Tribunal also hear appeals in those other security clearance areas — immigration and citizenship. To increase its expertise, the Security Appeals Tribunal should also review all screening reports that do not go to appeal, but which contain adverse information. These reports would be those which were sent to departments by the security intelligence agency or by the personnel security staffing officer, but which did not go to appeal because the Deputy Minister or agency head decided to grant the clearance, or the clearance was denied and the individual concurred with the reasons for denial. A review of these reports (about 500 a year) would provide the Security Appeals Tribunal with an overall view of the security screening information reported. The Tribunal would therefore not be hearing appeals in a vacuum but in the context of other adverse reports. The Tribunal should compile the results of these adverse reports and report on them annually to the Interdepartmental Committee on Security and Intelligence. In these annual reports, the Security Appeals Tribunal should bring to the attention of the government any changes it considers necessary in the security clearance process. The Tribunal, though not responsible for policy changes in this area, will have one of the best vantage points from which to assess the effectiveness and fairness of security screening procedures.

83. In our review of the security screening system, we were alarmed to find that there was no one organization charged with the responsibility of monitoring the system and initiating policy changes. One manifestation of this deficiency is the lack of a comprehensive, up-to-date set of statistics which would allow year by year comparisons of such important indicators as the number of people screened for each security classification, the number of adverse reports, and the number of individuals adversely affected by the screening procedures. We deal with the question of who should have responsibility for policy changes concerning security screening in Part VIII, Chapter 1. In essence, we shall recommend that the Cabinet Committee on Security and Intelligence should have ultimate responsibility here and that this Committee should designate a lead Minister to monitor and initiate policy changes in areas such as personnel security, physical security and emergency planning.

WE RECOMMEND THAT the federal government widely publicize any review and appeal procedures established for security screening purposes and that the Interdepartmental Committee for Security and Intelligence establish monitoring and control mechanisms to ensure that departments and agencies follow these procedures.

(128)

WE RECOMMEND THAT the Interdepartmental Committee for Security and Intelligence prepare for the approval of the Cabinet Committee on Security and Intelligence a set of internal review procedures for adverse security reports, to include at least the following points:

(a) the procedures must be comprehensive enough to include all individuals who might be adversely affected by security clearance procedures;

(b) decisions which adversely affect individuals for security reasons should be made by the Deputy Minister of the department concerned about the security problem;

(c) before making such a decision, the Deputy Minister should provide the individual in question with an opportunity to resolve the reasons for doubt;

(d) before making his decision, the Deputy Minister should consult appropriate officials in at least the Privy Council Office's Security Secretariat.

(129)

WE RECOMMEND THAT the federal government establish, by statute, a Security Appeals Tribunal to hear security appeals in the areas of Public Service employment, immigration, and citizenship. In the case of Public Service employment all individuals who have been or who suspect that they have been adversely affected by security screening procedures should have access to the Tribunal. The specific responsibilities of the Tribunal concerning Public Service employment should be as follows:

(a) to advise the Governor in Council on all appeals heard by the Tribunal;

(b) to review all adverse screening reports of the security intelligence agency and the Public Service Commission's security screening unit;

(c) to report annually to the Interdepartmental Committee on Security and Intelligence about its activities and about any changes in security clearance procedures which would increase either their effectiveness or their fairness.

(130)

WE RECOMMEND THAT

(a) the Security Appeals Tribunal consist of five members appointed by the Governor in Council, any three of whom could compose a panel to hear security appeals;

(b) the chairman of the Tribunal be a Federal Court Judge;

(c) the other members not be currently employed by a federal government department or agency.

(131)

WE RECOMMEND THAT the Security Appeals Tribunal disclose as much information as possible to the appellant and that the Tribunal have the discretion to decide what security information can be disclosed to the appellant.

(132)

WE RECOMMEND THAT the procedures of the Security Appeals Tribunal be similar to those now established for appeals against the dismissal from the Public Service or against deportation, with the added feature that members of the security intelligence agency or personnel security staffing officers be allowed to appear before the Tribunal to explain the reasons for denying a security clearance.

(133)

CHAPTER 2

IMMIGRATION SECURITY SCREENING

A. HISTORICAL BACKGROUND

1. Canada is a country mainly composed of immigrants or their descendants, but the desire to encourage immigration has become increasingly tempered by selectivity in deciding who will be permitted to immigrate. Statutory rejection criteria and screening procedures have been developed over the years to prevent the immigration of individuals deemed undesirable for occupational, medical, criminal, or security reasons. The numbers rejected for security reasons have always been negligible — less than one per cent of the total number of potential immigrants refused entry. Nevertheless, security rejections are sometimes highly controversial.

2. Without attempting a complete review of changes in security-related provisions of legislation relating to immigration, a brief survey of some of the more important changes is helpful. As early as 1872 there was a prohibition against immigrants who might be a security risk. That year an amendment to the Immigration Act provided that "The Governor-in-Council may, by proclamation, whenever he deems it necessary, prohibit the landing in Canada of any criminal, or other vicious class of immigrants, to be designated by such proclamation".[1] The Immigration Act of 1910 added to the prohibited classes: "... any person other than a Canadian citizen [who] advocates in Canada the overthrow by force or violence of the Government of Great Britain or Canada, or other British Dominion, Colony, possession or dependency, or the overthrow by force or violence of constitutional law or authority."[2] By 1923 immigrants were required to have visas, and procedures for the examination of visa applicants began to develop.

3. Following World War II, the Canadian government was anxious to meet domestic demands for labour, to facilitate family reunions and to contribute to the relief of displaced persons in Europe. Recognition of the security problem that this entailed led the Security Panel to recommend that the R.C.M.P. provide assistance to the Immigration Branch (at that time under the Department of Mines and Resources) in the screening overseas of prospective immigrants. This was not the first time the R.C.M.P. had been involved in immigration: during the Yukon gold rush, they filtered out ill-prepared prospectors and suspected criminals at the Chilkoot and White Passes. It was,

[1] S.C. 1872, 35 Vict. ch.28, s.10.
[2] S.C. 1910, Edw. VII, ch.27, s.41.

however, the first time that the R.C.M.P. had been asked to conduct such a service abroad.

4. In 1946, the first R.C.M.P. member was dispatched to London to join the immigration vetting team, but it was not until 1959 that the R.C.M.P. Act was amended to provide explicitly for such R.C.M.P. activity, by the addition of the phrase "outside of Canada" to section 4 of the Act.[3] As with the R.C.M.P.'s other screening functions — in citizenship, and Public Service employment — there was no specific statutory authorization for the role of the Force in immigration screening.

5. An Order-in-Council, made in June 1950, resulted in an increase in the flow of applications from the big European industrial areas. A huge backlog of cases awaiting security clearance developed because of the increase in the number of applications, and because many of the applicants were applying from countries in which they had not been resident for a sufficient period of time to permit the local authorities to provide the R.C.M.P. with adequate information. To reduce the workload, from time to time security screening was waived for various categories.

6. The Immigration Act of 1952[4] governed Canadian immigration procedures for the following 25 years. Section 5 of the Act listed the classes of persons who were prohibited from admission to Canada. The following were considered security risks:

> (l) persons who are or have been... members of or associated with any organization, group or body of any kind concerning which there are reasonable grounds for believing that it promotes or advocates... subversion by force or other means... except persons who satisfy the Minister that they have ceased to be members of or associated with such organizations, groups or bodies and whose admission would not be detrimental to the security of Canada;
>
> (m) persons who... are likely to engage in or advocate subversion by force or other means...
>
> (n) persons concerning whom there are reasonable grounds for believing they are likely to engage in espionage, sabotage or any other subversive activity...
>
> (q) persons who have been found guilty of espionage...
>
> (r) persons who have been found guilty of high treason or treason against or of conspiring against Her Majesty or of assisting Her Majesty's enemies in time of war,...

Section 19 of the Act (renumbered section 18 in the 1970 Revised Statutes of Canada), which was concerned with persons already in Canada, made subject to deportation, on security grounds, persons who fell within the following categories:

> (a) any person, other than a Canadian citizen, who engages in, advocates or is a member of or associated with any organization, group or body of

[3] S.C. 1959, ch.54.

[4] R.S.C. 1952, ch.325.

any kind that engages in or advocates subversion by force or other means of democratic government, institutions or processes, as they are understood in Canada;

(c) any person, other than a Canadian citizen, who, if outside Canada, engages in espionage, sabotage or any activity detrimental to the security of Canada;

7. In 1962, an Order-in-Council was passed introducing the principle of universal immigration to Canada for unsponsored applicants, although sponsored immigration remained geographically restricted.[5] In practice, immigration from countries where reliable information could not be obtained was restricted simply by providing no facilities for the processing of applications in such countries. By the mid-1960s, to meet urgent manpower needs, the Cabinet opened up immigration opportunities still further by accepting changes in security screening procedures. Automatic rejection criteria, such as Communist Party membership, were eliminated for the sponsored immigrant and the immigrant coming from a country controlled or influenced by the Communist Party. At the same time, easier international travel and a growing tourist industry led to a gradual removal of the visa requirement for most visitors. In 1967 an amendment to the Immigration Regulations allowed visitors to Canada to remain permanently, subject to only slightly more difficult selection criteria than those which applied to applicants abroad. It was considered at the time that not many persons would take advantage of that provision, but in fact thousands did so, and by 1970 one fourth of the landed immigrants were persons who first came to Canada as visitors.

8. The Immigration Appeal Board Act of 1967[6] created an appeal body independent of the Minister and extended the right of appeal for persons ordered deported, even at a port of entry. The Board was given power to set aside deportation orders on compassionate grounds. The very fact that a person was physically on Canadian soil determined his right of appeal, even if he had entered Canada illegally. An unintended consequence of this change was that it encouraged persons who might otherwise have had difficulty qualifying for immigrant status to come to Canada, ostensibly as visitors, but with the full intention of remaining. As such persons could now appeal deportation, the Immigration Appeal Board was soon swamped with up to 400 appeals a month. By the fall of 1970, a backlog of 4,000 cases had developed. Many of those who, had they applied abroad, might have been prohibited on security grounds from entering Canada as landed immigrants were thus able to remain, in effect, immune to deportation for a long period of time. Immigration Appeal Board procedures and departmental practice required that the appellants and their lawyers were to have access to all information submitted at special inquiries and appeal proceedings. Sometimes this could jeopardize security intelligence sources. If the R.C.M.P. refused to admit publicly that they had such information, the appellant won his appeal to remain in Canada. In cases where the appeal was based on compassionate or humanitarian grounds the

[5] *White Paper on Immigration*, 1964, section 95 "Security Screening", p. 36.
[6] S.C. 1966-67, ch.90.

alternative was that the Minister of Immigration and the Solicitor General would sign a certificate pursuant to section 21 of the Act, stating that in their opinion, based on confidential security reports, the Immigration Appeal Board must allow the deportation order or refusal of visa to proceed.

Recommendations of the Royal Commission on Security

9. In trying to resolve the dilemma between the need for security and the rights of the individual, the Report of the Royal Commission on Security, published in 1969, recommended both a tightening of security measures in relation to immigration and the establishment of clearer, more consistent security screening procedures for all categories of prospective immigrants. The recommendations of the Commission that have been at least partially implemented can be summarized as follows:

(a) *Changes in the role of the officers abroad*: The maturity, quality and training of both the R.C.M.P. and Immigration officers abroad should be upgraded so that normally individual cases could be decided jointly by these officers in the field. All cases of refusals for sponsored immigrants, and all cases where the officers in the field could not agree, should be reviewed in Ottawa by the Department of Manpower and Immigration and the Security Service, and, at the option of either, by the Security Secretariat in the Privy Council Office.

(b) *Universal screening procedures and guidelines* should be introduced for all prospective immigrants without regard for relationship, sponsorship or country of origin. Sponsors should also be screened. The same rejection criteria should apply to both sponsor and immigrant. New, universally applicable guidelines for rejection should be introduced.

(c) *Review procedures require modification*: Immigrants applying from within Canada should not be entitled to an appeal against rejection on security grounds. Sponsors whose relatives have been refused admission on security grounds should have access to a review of that decision by a security review board. Persons formally admitted as landed immigrants should not be subject to deportation without full judicial appeal before a body such as the Immigration Appeal Board.[7]

10. The first of these recommendations has been only partially implemented. In May 1975, after extensive interdepartmental consultation, the Solicitor General and the Secretary of State for External Afffairs, in an exchange of letters, agreed upon revised and expanded terms of reference for R.C.M.P. liaison officers abroad and contemplated a raising of their quality and status. When considering the rejection of an independent potential immigrant on security grounds, the liaison officer abroad confers with R.C.M.P. Headquarters before advising rejection to the Immigration officer in the field. The advice is normally accepted but in case of disagreement the Immigration officer at the foreign post can have the situation reviewed by Immigration Headquarters in Ottawa. When the R.C.M.P. liaison officer advises rejection of an immigrant

[7] *Report of the Royal Commission on Security*, 1969, paragraph 300.

sponsored by a permanent resident or citizen of Canada, the case is automatically reviewed by Immigration Headquarters in Ottawa.

11. The second recommendation has also only partially been implemented. New security screening guidelines have been introduced, universal in application but different in substance from those proposed by the Royal Commission on Security. Security screening is now required for nearly all immigrants between the ages of 18 and 70 except in certain tightly circumscribed cases of urgency, or for humanitarian considerations. These new security screening guidelines were approved by Cabinet in March 1975 at the same time as approval was given to what has come to be known as the Security Service's 'mandate'. These guidelines were essentially similar to that mandate, with two additions:

> Persons who hold, or have held, positions of executive responsibility in any organization, group or body which promotes or advocates the subversion, by force or violence or any criminal means, of democratic government, institutions or processes, as they are understood in Canada.
>
> Persons who engage in deliberate and significant misrepresentation or untruthfulness during any personal interview or in the completion of documents for immigration purposes, if such misrepresentation or untruthfulness has a bearing on background enquiries relating to admissibility to Canada.

12. The new guidelines served as the criteria for security screening and rejection until the Immigration Act, 1976, established the classes of people inadmissible to Canada for security reasons. Pursuant to section 19(1) of the Act these are:

> (e) persons who have engaged in or who there are reasonable grounds to believe will engage in acts of espionage or subversion against democratic government, institutions or processes, as they are understood in Canada, except persons who, having engaged in such acts, have satisfied the Minister that their admission would not be detrimental to the national interest;
>
> (f) persons who there are reasonable grounds to believe will, while in Canada, engage in or instigate the subversion by force of any government;
>
> (g) persons who there are reasonable grounds to believe will engage in acts of violence that would or might endanger the lives or safety of persons in Canada or are members of or are likely to participate in the unlawful activities of an organization that is likely to engage in such acts of violence;[8]

The Act also dealt with the deportation, on security-related grounds, of non-Canadian citizens already in Canada. Section 27(1) covered any permanent resident who

> (a) if he were an immigrant, would not be granted landing by reason of his being a member of an inadmissible class described in paragraph

[8] S.C. 1976-77, ch.52.

19(1)(c), (d), (e) or (g) or in paragraph 19(2)(a) due to his having been convicted of an offence before he was granted landing,

or

(c) is engaged in or instigating subversion by force of any government,

Section 27(2) dealt with any person, other than a Canadian citizen or a permanent resident who

(a) if he were applying for entry, would not or might not be granted entry by reason of his being a member of an inadmissible class other than an inadmissible class described in paragraph 19(1)(h) or 19(2)(c),

or

(c) is engaged in or instigating subversion by force of any government,

13. The differences between these statutory security criteria and those of the 1952 Immigration Act reflect the change in the international environment. Concerns with treason and wartime activities against Her Majesty's allies have shifted to acts of violence and terrorism. Any likelihood of an act of violence, whether or not politically motivated, which might endanger the safety of Canadians, is now a ground for rejection.

14. In 1972, changes in the Immigration regulations were passed which were designed to eliminate the practice of applying for landed status from within Canada. However, visitors and persons on student and temporary work visas who had relatives in Canada continued to apply, many of them successfully. In 1973 the Immigration Appeal Board Act was amended to remove the right of appeal from all but permanent residents, refugees, persons in possession of visas, and Canadian citizen sponsors.

15. That part of the third recommendation of the Royal Commission on Security, which proposed that permanent resident deportation cases involving security should be heard by the Immigration Appeal Board, was not accepted. Instead, under section 42 of the Immigration Act, 1976, a new advisory review body, the Special Advisory Board (S.A.B.), was created:

(a) to consider any reports made by the Minister and the Solicitor General pursuant to subsection 40(1); and

(b) to advise the Minister on such matters relating to the safety and security of Canada... as the Minister may refer to it for its consideration.[9]

16. This Board is in some ways similar to the Security Review Board proposed by the Royal Commission on Security. However it does not hear

[9] *Ibid.* Subsection 40(1), considered later in the text, reads as follows:

40. (1) Where the Minister and the Solicitor General are of the opinion, based on security or criminal intelligence reports received and considered by them, that a permanent resident is a person described in subparagraph 19(1)(d)(ii), or paragraph 19(1)(e) or (g) or 27(1)(c), they may make a report to the Chairman of the Special Advisory Board established pursuant to section 41.

sponsored immigration rejection cases, but rather acts as adviser in these cases to the Minister responsible for Immigration. Under section 42(a) it does hear evidence in cases concerning permanent residents whom the Minister of Employment and Immigration and the Solicitor General are seeking to have deported on security grounds where the public disclosure of such evidence would endanger national security. The S.A.B. has received only one report made by the Minister and the Solicitor General under section 40(1). It has acted in its security advisory function under section 42(b), advising the Minister on contentious security screening cases.

Special immigration security procedure

17. In the decade that followed the report of the Royal Commission on Security, the staging of the Summer Olympic Games in Montreal in 1976 had a permanent effect on immigration security policy and procedures. Provisions similar to those contained in the Temporary Immigration Security Act, which allowed visitors to be turned back at a port of entry or deported without a formal inquiry, have been incorporated into the Immigration Act, 1976, but modified to provide for a hearing by a departmental adjudicator.

The Immigration Act, 1976

18. The new Immigration Act, passed in 1977, came into force in April 1978. It reflected a 1975 Green Paper suggestion that immigration legislation should embody a more positive approach. The negative 'gate keepers' stance of previous legislation was replaced by a more positive emphasis on the reasons and means for admittance; only two of the 10 immigration objectives stated in section 3 of the Act are concerned with safeguarding public order and security. As one commentator noted, the legislation

> ... attempts to strike a balance between administrative efficiency and respect for civil liberties. It accords the government increased power to deal with terrorists, subversives, criminals and those seeking to circumvent immigration laws; at the same time, it offers increased protection to the individual in a number of areas — refugees, the adjudication system, alternatives to deportation, and arrest and detention.[10]

19. We now turn from this chronology, which has attempted to place present immigration security policy in a historical perspective, to a critical analysis of the present system of immigration security screening, including its scope, the criteria for security rejection, the role of the R.C.M.P. in the screening process, and the appeal mechanisms available.

B. THE EXTENT OF IMMIGRATION SECURITY SCREENING

20. The screening of aliens crossing a national frontier can still be considered the first line of defence in a country's security programme, but in today's fast-shrinking world it is a decreasingly effective barrier. Given this changing

[10] Warren Black, "Novel Features of the Immigration Act, 1976" (1978) 56 *Can. Bar Rev.*, 56.

situation, should there continue to be security screening of people who wish to visit or immigrate to Canada? We feel that the answer to this question must be in the affirmative. A total elimination of security screening of applicants would not be desirable for this country, since Canada is likely to maintain relatively high levels of immigration in the future. Moreover, unlike many European countries, Canada does not have an extensive system of internal controls, with flexible deportation procedures and extremely stiff citizenship requirements, making it relatively easy to remove undesirable foreigners.

21. As we indicated earlier, nearly all persons between the ages of 18 and 70 wishing to immigrate to this country are subject to security screening. While there appears to be no reason to modify the universal nature of the screening for potential permanent residents, there are some problems with the selectivity of the screening for visitors and refugees.

Permanent residents

22. There is one change in the screening for permanent residents that should be considered. The practice should provide that the security liaison officer abroad is involved in the process of deciding whether screening should be waived on humanitarian grounds.

Visitors and temporary residents

23. There are at present two situations in which persons coming to Canada as visitors or temporary residents must undergo a security screening process. They are if a person is from a country whose citizens require a visa to visit Canada, or if a person arrives in Canada and then applies for permanent resident status. Visas are not required to enter Canada except in the case of citizens of certain designated countries. All individuals applying for visas to come to Canada from these countries require screening by the R.C.M.P. Security Service. For citizens of other countries there is normally no security screening of applicants for temporary permits unless an applicant has a record of refusals from the post abroad or the applicant's name appears in the Immigration Index of individuals whose entry into Canada is undesirable for security reasons.

24. In the past the Security Service has insisted on applying the same screening criteria to applicants for visitor's visas as are applied to applicants for permanent residence, even though the holder of a visa may be visiting Canada for a very short period of time. One reason for this practice is that a great many visitors and holders of permits (commonly referred to as Minister's permits) apply for permanent status after they arrive in Canada. For instance, 14,288 of the 111,899 persons granted permanent residence status in 1979 arrived in Canada as visitors or on Minister's permits. The screening prerequisites when an individual applies from within Canada are the same as for a person applying from abroad, but if an applicant already in Canada does not pass the security requirements, the Minister is then faced with the option of deportation, with a possible public outcry, or waiving the security objection. Another reason that the Security Service has applied screening criteria to visa applicants which are identical to those which are applied to applicants for

permanent residence is that some temporary residents prolong their stay in Canada by repeatedly having their visitor's status in Canada extended.

25. We think it is inappropriate to apply security criteria in exactly the same way to temporary visitors as to applicants for permanent residency. The reasons for the existing practice, in our view, can be satisfied by two changes in procedure. First, when the security intelligence agency has information about an individual which would justify his rejection if he were an applicant for permanent residency but not justify denying him the right to visit Canada for a limited period, then a non-renewable visa should be issued. Second, those who have obtained temporary permits and have not been screened should be subjected to normal security screening if they apply for a renewal of their visa. Applications for renewal could be sent to the security intelligence agency for a records check (and to the R.C.M.P. for a criminal records check). Alternatively, a less thorough but possibly less costly system would be one of 'stop-notices'. A visa would not be extended automatically if the security intelligence agency has notified Immigration officials that a temporary resident is a security risk. There is already provision for a system similar to this 'stop-notice' procedure in the Immigration Act. Under section 27(2) of the Act reports can be written to the Deputy Minister of Employment and Immigration when a temporary resident has been engaging in criminal or subversive activities.[11]

Refugees

26. The desire to deal expeditiously and humanely with large numbers of homeless and persecuted refugees has inevitably meant a relaxation of security screening requirements.

27. Canada has gained a humanitarian image internationally because of the large number of refugees it accepts. For example, Canada accepted twice as many Chilean refugees as any other two countries combined. Canada's receptiveness to the victims of political repression is reflected in the Immigration Act, 1976, in which the refugee is designated a separate class for whom special admission standards may be established. Following the United Nations Convention and Protocol Relating to the Status of Refugees, the Immigration Act, 1976, defines a Convention Refugee as any person who cannot return to his own country

> by reason of well-founded fear of persecution for reasons of race, religion, nationality, membership in a particular social group or political opinion.[12]

28. The Immigration Act, 1976, provides for flexible procedures in which each refugee situation can be treated on its merits. Under sections 6(2) and 115(1)(e) of the Act special regulations can be written to facilitate the entry into Canada of a particular group of refugees or quasi-refugees. While these procedures cannot override the definition of inadmissible classes in section 19, they can provide for a modification of the way in which the security criteria are applied. While such flexibility is desirable, there is a danger that in the turbulent atmosphere of an international crisis, decisions might be made to

[11] S.C. 1976-77, ch.52.
[12] *Ibid.*

reduce screening without an adequate consideration of the implications for the security of Canada.

29. We think it is possible to retain the humanitarian and flexible procedures now established while at the same time reducing the potential risk inherent in accepting large numbers of refugees as immigrants. The Contingency Refugee Committee should be reinstated as a special task force under the Interdepartmental Committee on Security and Intelligence to ensure that there is a continuing and current assessment of potential refugee situations, ready for use by the government. The security intelligence agency should contribute to this committee. In co-operation with other government departments and agencies, it should help to prepare security profiles of countries which appear likely to generate refugee situations. Then, if a crisis occurs, the government could take time to balance humanity and security in making its decisions.

30. Convention Refugees should not routinely be subjected to a security screening interview on arrival in Canada even if they have not been subjected to the full security screening process abroad.

31. Another reason for prohibiting routine screening interviews of Convention Refugees after their arrival in Canada is that the information might be used for other purposes.

WE RECOMMEND THAT the security intelligence liaison officer at the post abroad be involved in any decision, on application for permanent residency, to waive immigration security screening for humanitarian reasons or in cases of urgency.

(134)

WE RECOMMEND THAT the security screening rejection criteria applied to visa applicants reflect the temporary nature of their stay. Where appropriate, non-renewable visas should be issued for applicants who could not pass the security criteria for permanent immigration.

(135)

WE RECOMMEND THAT applicants for the renewal of temporary permits or visas be required to undergo the security screening process.

(136)

WE RECOMMEND THAT the humanitarian and flexible procedures for dealing with Convention Refugees remain, but that the security intelligence agency, in co-operation with other government departments and agencies, help prepare regular threat assessment profiles of potential refugee situations for the Contingency Refugee Committee, which should be revived.

(137)

WE RECOMMEND THAT the security intelligence agency, hold security screening interviews with Convention Refugees after their arrival in Canada, not as a matter of course, but only for cause.

(138)

C. IMMIGRATION SECURITY CRITERIA

32. As we have seen, the Immigration Act, 1976, introduced new definitions of the classes of persons to be denied admission to Canada on security grounds.

These new statutory security criteria (set out in full in section A of this chapter) are too broad, and are inconsistent with the definition of threats to the security of Canada which we proposed earlier in this Report should be the basis of the statutory mandate of the security intelligence agency.

33. It could be argued that because screening for immigration purposes is our first line of defence, the security rejection criteria should be more extensive than those for other screening functions. We do not agree. If the criteria governing immigration screening are wider than those which define the basic mandate of the security intelligence agency, the agency will, in effect, be authorized to seek intelligence from foreign agencies that it is not empowered to collect in Canada. This would violate one of the principles which we have recommended should govern the security intelligence agency's relations with foreign agencies. Therefore, to avoid ambiguity and inconsistency, we recommend that the Immigration Act be amended so that the criteria for denying admission to Canada on security grounds are consistent with the definition of threats to the security of Canada found in the statutory mandate of the security intelligence agency.

34. There is a need for administrative guidelines to interpret the statutory criteria and designate specific areas of security concern. There have been three separate sets of such guidelines approved by Cabinet in the past. The existing guidelines, established prior to the Immigration Act, 1976, are in some respects inconsistent with the new statutory criteria. They should be made consistent with the proposed amended statutory criteria.

35. Administrative guidelines of this kind should be subject to a process of periodic review and adjustment in order to reflect changes in the perception of security threats. This did not always happen in the past. It took nearly 20 years before the guidelines differentiated between the security risk entailed by Communist Party membership in the Communist bloc countries and those of western European countries. Participation in political violence abroad, especially, requires careful analysis: the context in which the violence took place is important in any consideration of whether an individual would constitute a risk to the security of Canada. Carefully drafted guidelines should assist the security intelligence agency to determine what is pertinent for immigration security clearance purposes.

WE RECOMMEND THAT section 19(1)(e), (f) and (g) of the Immigration Act be repealed and the following substituted:

19. (1) No person shall be granted admission if he is a member of any of the following classes:

(e) persons who it is reasonable to believe will engage in any of the following activities:

(i) activities directed to or in support of the commission of acts of espionage or sabotage;

(ii) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(iii) **political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.**

(iv) **revolutionary subversion, meaning activities directed towards or intending ultimately to lead to the destruction or overthrow of the liberal democratic system of government.**

(139)

WE RECOMMEND THAT administrative guidelines to interpret the statutory classes of persons denied admission to Canada on security grounds be drafted for Cabinet approval.

(140)

D. ROLE OF THE SECURITY INTELLIGENCE AGENCY IN IMMIGRATION SCREENING

36. R.C.M.P. liaison officers are stationed at 28 Canadian posts abroad. These officers are responsible, amongst their other duties, for the security vetting of all applicants for permanent immigration to Canada. Liaison officers check the records at the post and request criminal and security information from the local police and security intelligence agencies, and at times from other foreign agencies, and assess the security relevant information.

37. There is a danger in the immigration screening process of placing too great and uncritical reliance on foreign agency information. The information received must always be carefully analysed in the context of the political circumstances of the country providing it. No foreign agency should be considered a 'reliable source' in the sense that its reports can be accepted uncritically. The interests and perceptions of foreign nations will often differ from those of Canada, and their interpretation of data may well reflect those differences. The security intelligence agency liaison officers and the analysts at Headquarters must be sensitive to the shades of difference between foreign and Canadian concerns. One of the reasons an effective and knowledgeable review body is needed to review the evidence supporting denials of security clearance in immigration cases is the fact that frequently the evidence will be based on reports from foreign agencies.

38. The security and criminal intelligence required to determine whether the criteria of the Immigration Act are met is not always available. There are several countries, for instance, that do not permit the reporting of criminal information about their citizens to any foreign agency. To authorize the Canadian security intelligence agency to establish a paid source or otherwise to break the laws of a foreign country to obtain the required screening intelligence in those countries would be unacceptable. In these situations Canada should endeavour to establish arrangements for obtaining the intelligence through government to government negotiations. If inter-governmental agreement cannot be reached, the onus should be placed upon the immigrant, personally, to provide the Canadian immigration officials with documentation guaranteeing that he or she has no criminal record, or as in the case with immigration

from Communist countries where security intelligence is not available, the requirement of intelligence for the particular criteria in question could be waived.

WE RECOMMEND THAT officers from the security intelligence agency carry out immigration security screening functions abroad. If they are tasked to obtain criminal and other intelligence pertinent to the suitability of an immigrant, they should pass it on to the Immigration Officer for assessment.

(141)

WE RECOMMEND THAT the security intelligence agency cross-check immigration screening information received. The security intelligence agency should assess the information on potential immigrants received from a foreign intelligence agency in the light of the political concerns and interests of the country of the providing agency.

(142)

WE RECOMMEND THAT the security intelligence agency not be authorized to transgress the laws of foreign countries in order to obtain intelligence for immigration screening purposes.

(143)

E. IMMIGRATION APPEAL PROCEDURES

39. Immigration appeal procedures deal with appeals against certain removal orders and decisions refusing applications for or by sponsored (family class) immigrants. The Immigration Appeal Board (I.A.B.) hears such appeals against removal orders and decisions made by the Canada Employment and Immigration Commission. The I.A.B. can determine appeals based on questions of fact or of law and also has power to overturn a removal order or decision if it considers that there are humanitarian grounds for doing so. However, according to section 83(1) of the Immigration Act, 1976, the I.A.B. cannot overturn a removal order on humanitarian grounds or a sponsored immigrant application refusal on any grounds if the Minister of Employment and Immigration and the Solicitor General co-sign and file a certificate with the Board "stating that, in their opinion, based on security or criminal intelligence reports... it would be contrary to the national interest for the Board..." not to dismiss the appeal.[13]

40. In our opinion the criterion of "contrary to the national interest" used in section 83(1) is not appropriate to decide matters involving security. The words are too vague and imprecise. We think that with respect to security matters the phrase used ought to be "contrary to national security", and this phrase should be defined as having the same meaning as we have recommended for the definition of threats to security in the statute governing the security intelligence agency. This would be consistent with the wording in section 40(9) of the Act which covers similar appeals with respect to permanent residents.

41. Pursuant to section 39 of the Immigration Act, 1976, in security cases involving any person other than a permanent resident or Canadian citizen, a

[13] *Ibid*, s.83(1).

person may be ordered deported by certain immigration officials if the person is named in a certificate signed by the Minister of Employment and Immigration and the Solicitor General and the certificate is filed with the official stating that "in the opinion of the Minister and the Solicitor General, based on security or criminal intelligence reports. . . which cannot be revealed in order to protect information sources..."[14] the person falls within the categories described in paragraph 19(1)(d), (e), (f) or (g) or paragraph 27(2)(c) of the Act. Four such certificates, which are conclusive, were signed and filed in each of 1978 and 1979.

42. The provisions of section 39 of the Act do not apply to Canadian citizens or permanent residents. When the deportation of a permanent resident is proposed on security grounds, and the evidence cannot be presented at an open inquiry, a different procedure is followed: a report under section 40(1) of the Act is made by the Solicitor General and the Minister of Employment and Immigration to the Chairman of the Special Advisory Board. Section 40(1) reads:

> 40. (1) Where the Minister and the Solicitor General are of the opinion, based on security or criminal intelligence reports received and considered by them, that a permanent resident is a person described in subparagraph 19(1)(d)(ii), or paragraph 19(1)(e) or (g) or 27(1)(c), they may make a report to the Chairman of the Special Advisory Board established pursuant to section 41.

43. The Special Advisory Board, as we noted in section A of this chapter, has two functions, one of which is considering reports by the Ministers alleging a permanent resident's deportability on security grounds based on confidential evidence. Upon receiving such a report the Board follows an appeal procedure similar to that used by a Commissioner appointed under the Public Service Security Inquiry Regulations to deal with security dismissals from the Public Service. The Special Advisory Board in dealing with a report, can request all relevant information and can

> determine what circumstances and information should not be disclosed on the ground that disclosure would be injurious to national security or to the safety of persons in Canada.[15]

The Board may decide at any time that there is nothing in the information before it the disclosure of which would endanger "national security or the public safety of persons in Canada",[16] and in such a case it must terminate its proceedings so that the case can be heard through the regular channels of inquiry and appeal to the I.A.B. or the Federal Court.

44. Under section 40(4) of the Immigration Act, when the Board has determined what information can be disclosed to the individual concerned, it notifies him of the proposal to deport him and informs him as fully as possible about the circumstances and the nature of the allegations. The individual has the right to a hearing, to be held *in camera*. He has the right to be represented

[14] *Ibid.*, s.39.
[15] *Ibid.*, s.40(2)(b).
[16] *Ibid.*, s.40(8).

by counsel, to call witnesses and to present evidence. At the conclusion of the hearing the Special Advisory Board makes a report to the Governor in Council, for consideration as to whether to make a deportation order. In our view this role of the Special Advisory Board should be transferred to the Security Appeals Tribunal which we recommended should be created.

45. There is a further appeal route for all persons faced with deportation. Section 28 of the Federal Court Act[17] allows an appeal directly to the Federal Court, bypassing the I.A.B. In such an appeal against deportation, where the deportation order had been made on sensitive security grounds, an appellant would likely encounter substantial difficulty, either because the Solicitor General would object to the production of evidence by signing an affidavit under section 41(2) of the Federal Court Act, or because the provisions of section 119 of the Immigration Act would be invoked. Section 119 reads:

> 119. No security or criminal intelligence report referred to in subsection 39(1), 40(1) or 83(1) may be required to be produced in evidence in any court or other proceeding.[18]

46. We do not feel that an appeal to the Federal Court of Canada is the most appropriate way of reviewing the security aspects of deportation cases involving persons who are neither citizens nor permanent residents. In such cases a section 39 certificate is more than a ministerial affidavit certifying that a document contains evidence that would be injurious to national security; it is "proof of the matter therein", i.e. that, based on security or criminal intelligence reports, the person meets the criteria in the Act for rejection or deportation. We think that the most appropriate agency for reviewing the reports relied upon in the exercise of ministerial power under section 39, is the Security Appeals Tribunal with its expertise in security matters and full access to security reports. As we recommend above, this Tribunal should absorb the functions of the Special Advisory Board in relation to appeals of permanent residents. In this way the proposed Tribunal will combine the functions of appeal for both permanent and non-permanent residents. We are not recommending that individuals be given a right to appeal personally to this body — only that there should be some independent review of the evidence. The same review body that examines deportation orders against permanent residents should be responsible for this review. In that way there will be consistency in decisions and an experiential base to draw upon.

47. The Security Appeals Tribunal should also review all cases in which, although the security intelligence agency has recommended deportation or denial of admittance or status, the responsible Minister has chosen not to follow the advice. As with recommended denials of security clearance for the public service, this review function will help to inform the Security Appeals Tribunal of the rejection procedure as a whole.

WE RECOMMEND THAT the criteria in s.83(1) of the Immigration Act, as far as they relate to security matters, be amended to read "contrary to national security".

(144)

[17] R.S.C. 1970, ch.10 (2nd Supp.).
[18] S.C. 1976-77, ch.52.

WE RECOMMEND THAT the responsibilities of the Special Advisory Board under subsection 42(a) of the Immigration Act be transferred to the proposed Security Appeals Tribunal.

(145)

WE RECOMMEND THAT the ministerial certificates for the deportation of temporary residents and visitors continue to be considered as proof, and hence not subject to appeal, but that the security or criminal intelligence reports upon which the deportation decision is based should be subject to independent review by the same body that reviews the evidence in the case of permanent residents, namely the Security Appeals Tribunal.

(146)

WE RECOMMEND THAT the Security Appeals Tribunal review all the security reports written by the security intelligence agency where the recommendation for deportation or denial of permanent residency status or admittance was not followed by the Minister.

(147)

CHAPTER 3

CITIZENSHIP SECURITY SCREENING

A. HISTORICAL BACKGROUND

1. The granting of Canadian citizenship can no longer be considered a privilege bestowed by prerogative of the Crown. Successive legislation has made the granting of citizenship the responsibility of the Citizenship Courts. Citizenship is a right that can be claimed after three years by any immigrant, 18 years or older, who has been legally admitted into Canada on a permanent basis, who has an adequate knowledge of Canada and one of its official languages, and who is not subject to a list of specific prohibitions (for example, an immigrant who is an inmate in a penitentiary cannot become a Canadian citizen). For reasons of security and public order, however, the government still retains discretionary power to reject an applicant for Canadian citizenship.

2. For almost 50 years, the R.C.M.P. has been supplying the government with security and criminal information on citizenship applicants. Under the Naturalization Act of 1914 an arrangement was established between the R.C.M.P. and the Department of the Secretary of State. By World War II, the R.C.M.P. was systematically investigating the character and background of all applicants for what was then called naturalization. Criminal and subversive indices were checked, an interview was held with each applicant, and reports were sent to the Department of the Secretary of State. The Canadian Citizenship Act of 1947 made no explicit provision for the security screening; the practice that had developed through the years continued under section 10(1)(d), which required that an applicant for citizenship be "of good character".[1] Under this Act, the Minister was given final authority to approve or deny an application for citizenship.

3. In January 1951, an interdepartmental Citizenship Advisory Committee, consisting of representatives from External Affairs, Citizenship, and the Privy Council Office, with the R.C.M.P. as observers, was established. The Committee began to examine all adverse reports submitted by the R.C.M.P. and to advise the Minister whether a citizenship certificate should be granted. The following month, Cabinet agreed upon criteria for the rejection of citizenship on security grounds. An applicant described as a member of a Fascist, Communist or other revolutionary organization would be rejected, as would applicants who were members of a Communist front organization.

[1] S.C. 1946, ch.15.

4. Heavy immigration in the late 1940s and early 1950s affected the citizenship screening procedure. The R.C.M.P. could not process what amounted to a threefold increase in citizenship applications. As a result, in 1954, the criminal records check was eliminated. Less than one per cent of enquiries turned up evidence of a criminal record, and it was felt that the examination by the Citizenship Judge, local knowledge of the individual in smaller communities, information received from Clerks of the Court and other interested parties, together with the reports received from the Immigration Branch, would identify most individuals who might have criminal records.

5. A more lenient attitude to the granting of citizenship developed in the early 1960s and steps were taken to reduce the detail involved in the application of security criteria.

6. The Royal Commission on Security concurred with the trend to reduce the stringency of the citizenship security criteria. The Commission's Report concluded that possession of citizenship only marginally increased the capabilities of a Canadian resident in the field of espionage and subversion.[2] Hence, the Commissioners argued, there is "an element of unfairness in denying citizenship to an individual who has been a resident of Canada for five years when his actions have not been illegal and represent no immediate and direct threat to the security of Canada."[3]

They suggested that:

> ... as a general rule citizenship should be withheld only for actual illegalities or criminal acts; in the area of security, these would include espionage, treason and similar offences. Membership in communist organizations or even of the Party itself, however, should not constitute causes for rejection.[4]

7. Nevertheless, the Commission thought that despite this general rule there would be some cases in which the applicant would constitute a significant risk to security, even though not involved in an illegal activity. In such cases the Minister should exercise discretion in refusing citizenship on security grounds. The Report recommended that:

> ... the grant of citizenship should normally be refused on security grounds only if actual illegalities or criminal acts have been committed and proved in court, and not merely for membership in subversive associations or even the Communist Party. However, WE RECOMMEND that ministerial discretion should be retained to deal with certain cases in which it may remain appropriate to withhold citizenship for particularly significant security reasons. All persons whose applications are rejected on security grounds should have access to the Security Review Board.[5]

8. "Significant security risk" was left undefined by the Royal Commission except in the negative sense that the category did not include those who merely hold "membership in subversive associations or even the Communist Party."[6] The Commission's recommendation was therefore difficult to implement. The

---

[2] *Report of the Royal Commission on Security*, 1969, paragraph 154.
[3] *Ibid.*, paragraph 155.
[4] *Ibid.*
[5] *Ibid.*, paragraph 301.
[6] *Ibid.*

Cabinet finally decided in 1973 that security clearance should remain a requirement for obtaining citizenship. The Interdepartmental Committee on Citizenship (formerly the Advisory Committee on Citizenship) drew up a new list of criteria, which, although never formally approved by Cabinet, remained until recently the basic working criteria for citizenship security screening. According to those criteria the R.C.M.P. were to report:

(1) Persons known or strongly suspected to be involved in espionage activities.

(2) Persons known or strongly suspected to be terrorists.

(3) Persons actively engaged or prominently involved with violence-prone organizations.

9. The new Citizenship Act was assented to by Parliament on July 16, 1976, and proclaimed on February 15, 1977.[7] Although there was no specific mention of screening, the new Act had a direct effect on the R.C.M.P. Security Service. Sections 19 and 20 dealt with probation and criminal records, while section 18 was concerned with security. Subsection 18(1) reads as follows:

> 18. (1) Notwithstanding anything in this Act, a person shall not be granted citizenship under section 5 or subsection 10(1) or be issued a certificate of renunciation under section 8 if the Governor in Council declares that to do so would be prejudicial to the security of Canada or contrary to public order in Canada.

10. Since the Act came into effect, the Security Service has again undertaken criminal records checks for all applicants for citizenship and the Interdepartmental Committee, now called the Interdepartmental Advisory Committee on Citizenship, has begun to meet again. This Committee has drawn up new screening criteria, which were ratified by Cabinet in December 1979. Before examining these criteria we turn to an evaluation of the present citizenship screening procedures.

B. THE ROLE OF A SECURITY INTELLIGENCE AGENCY IN CITIZENSHIP SCREENING

11. In 1979, the Security Service carried out subversive and criminal records checks on each of the 130,000 applicants for Canadian citizenship. Although the results suggested a seemingly low return for the effort expended, the efficacy of the citizenship screening programme must be evaluated in the context of the protection it affords the security of Canada. Likely, knowledge that there is a screening process is in itself a deterrent to applications by those who suspect that they will be rejected on security grounds.

12. We agree with the Royal Commission on Security that the security risk in granting citizenship is marginal, yet it must be noted that a Canadian citizen cannot be deported, except under the War Measures Act. Thus, if citizenship is granted to an individual engaged in activities considered threatening to the

[7] S.C. 1977-78, ch.22.

security of Canada that person can virtually never be deported. Moreover, a Canadian passport provides the possibility of travelling to most parts of the world; hence, advantage could be taken of a Canadian passport to facilitate either international terrorism or espionage activities. Furthermore, security implications accompany some of the rights and opportunities afforded a Canadian citizen in the approximately 90 federal statutes and more than 500 provincial statutes that contain references to the requirements or privileges dependent on citizenship. These restrictions to some extent protect various internal processes critical to our democratic state. For instance, only Canadian citizens can legally vote or run for office in federal, and some provincial and municipal elections, and a number of professions, including the law societies of the provinces, require citizenship.

13. These security ramifications of the granting of citizenship may be minor but they establish a need to retain the discretionary power, found in the Citizenship Act, to reject application for citizenship on security grounds. We agree with the Royal Commission on Security that normally a person should not be rejected for security reasons unless an actual illegality or criminal act has been committed. Further, we feel that, if an individual is seen to be a serious security risk, deportation, rather than the rejection of citizenship, should ensue. As we discussed in Chapter 2 of this part of the Report, in the past, deportation of persons reported to be security risks was difficult as it required a public hearing. Because members of the Security Service, anxious to protect the source of their information, were often reluctant to present their evidence at these public deportation hearings, deportation could not proceed. Under the Immigration Act of 1976 these deportation difficulties have been rectified. There is provision for reporting security risks (section 27(1) and (2)), for the deportation of non-permanent residents without appeal (section 39) and for *in camera* hearings by a Special Advisory Board for the deportation of permanent residents (section 40).[8] Given these changes, we feel that the security intelligence agency should report relevant security information concerning permanent residents applying for citizenship, not only to the Citizenship Branch but to the proper Immigration authorities, for the purpose of deportation. Deportation is a much more effective means of counteracting a significant security problem than is rejection of citizenship. If the threat posed by the applicant is not sufficient to warrant deportation, yet still of significant concern, the security intelligence agency should send a report to the Registrar of Citizenship for rejection purposes.

14. The R.C.M.P. Security Service has no formal authorization to screen applicants for Canadian citizenship. The origins of the procedure, now obscure, were developed some time prior to the passage of the 1947 citizenship legislation. The 1975 Cabinet Directive on the Role, Tasks and Methods of the R.C.M.P. Security Service did not mention citizenship screening or any of the other screening functions of the R.C.M.P. Other Cabinet Directives authorize security screening for classified positions in government and for immigration, but in the case of citizenship no such formal directive exists. Formal authoriza-

[8] S.C. 1976-77, ch.52.

tion is needed for the security intelligence agency's role in providing information about applicants for citizenship who might threaten the security of Canada. This authorization should be included in the statutory mandate given the security intelligence agency.

15. The citizenship security screening procedure now in place is cumbersome. Many hours of routine paperwork are required within the Citizenship Registration Branch of the Secretary of State's Department and within the Security Service to check all citizenship applications against Security Service records. When adverse information is found, the Security Service screening officer discusses the case with intelligence officers concerned with that area of subversive activity. If the case is considered of significant security concern, an adverse report is written to the Citizenship Registration Branch.

16. Despite its cumbersome quality, we recommend that the procedure be retained. We have considered recommending other procedures, such as having the security intelligence agency assess citizenship rejection in the same manner as it now assesses the possibility of deportation. When an individual, otherwise eligible for citizenship, comes to the attention of the agency, an assessment could be made as to whether the rejection of citizenship is warranted. If so, the individual's name could be sent to the Citizenship Registration Branch. When such a person applies for citizenship, the name would be found on the list and the Citizenship Registration Branch would notify the security intelligence agency. The agency would then evaluate the case and decide whether or not to recommend denial of citizenship on security grounds. This procedure would involve an active analysis of information and as such, we feel, would be more appropriate for a security intelligence agency than the passive and routine processing of thousands of files such as is involved in the current citizenship security screening programme. Nevertheless, on balance, we have decided that the present system is preferable. The alternative which we considered would require the security intelligence agency to supply the Citizenship Registration Branch with a list of names, and there is always the danger that such a list would not be secure. Leakage of the names on the list could result in unnecessary damage to the reputations of the individuals implicated or to current operations of the security intelligence agency.

17. While the procedure is cumbersome, the cost of the present programme is not a serious factor. The annual cost is approximately $163,000, or $1.30 per case.[9] The present system, moreover, allows a screening of all citizenship applicants, which ensures that the security intelligence agency is aware of applications for citizenship by anyone about whom they have an active concern. Finally, the deterrent effect alone of such a universal screen may be sufficient grounds for keeping the procedure in place. Residents, otherwise eligible, may refrain from applying for citizenship if they believe that in so doing their activities will be reviewed by the security intelligence agency.

18. A Security Service citizenship screening procedure that should be discontinued is the check of criminal records. Not only is the present procedure

[9] This is the combined figure from both the R.C.M.P. and Citizenship Registration Branch, $98,000 from the former and $65,000 from the latter. It includes both man-hours and postage.

inefficient but it is outside the function of a security intelligence agency. In 1954, the R.C.M.P. stopped routine criminal records checks because criminal information on citizenship applicants could be obtained from immigration statistics and other sources. This system of criminal records checks should be reinstated. Information on the criminal activity of permanent residents is centralized for deportation purposes within the Canada Employment and Immigration Commission (for the purpose of 'section 27(1) reports'). Notification, applicable for three years, on such individuals could be supplied to the Citizenship Branch by the Enforcement Branch of Immigration. The procedure would be similar to the deportation notices already sent by the Immigration Regional Offices to fulfill the requirements of section 5(e) of the Citizenship Act.

19. Screening of citizenship applicants is a service provided by the Security Service to government. As we noted in Part V, Chapter 6, we have heard evidence as to one case in which the Security Service provided this service in a questionable manner. In this case the security objection was waived unilaterally by the Security Service without informing the other departments of government, so that citizenship would be granted, the aim being to discredit the applicant's standing with a foreign intelligence service (Vol. 171, pp. 123484-89; Vol. 172, pp. 123507-13). It is possible that at times one security concern may override another; however, we feel that in such circumstances the security intelligence agency should inform its Minister, who should in turn inform the Minister responsible for citizenship. The security intelligence agency should not unilaterally deviate from the citizenship rejection criteria.

WE RECOMMEND THAT the discretionary power of the Governor in Council to reject citizenship on security grounds be retained. Upon receiving a request for citizenship screening, the security intelligence agency should report any significant security information, not only to the Citizenship Registration Branch for the rejection of citizenship, but also to the appropriate immigration authorities for deportation purposes.

(148)

WE RECOMMEND THAT the security intelligence agency continue to screen all citizenship applicants.

(149)

WE RECOMMEND THAT the security intelligence agency no longer process criminal record checks on citizenship applicants.

(150)

WE RECOMMEND THAT when the security intelligence agency feels that a competing security concern should take precedence over its security screening role in citizenship the Minister responsible for the security intelligence agency and the Minister responsible for the citizenship security clearance should be informed.

(151)

C. CITIZENSHIP SECURITY CRITERIA

20. There are several different levels of citizenship security rejection criteria. At the most general level, section 18(1) of the Citizenship Act states that citizenship is not to be granted if "the Governor in Council declares that to do

so would be prejudicial to the security of Canada or contrary to the public order in Canada".[10]

21. In 1960, membership per se in Communist front organizations was no longer considered cause for rejection. The Royal Commission on Security in 1969 also recommended that membership in the Communist Party itself should not be grounds for rejection. In 1973, the Interdepartmental Committee on Citizenship drew up new rejection guidelines, in which three criteria — espionage, terrorism and membership in violence-prone organizations — were mentioned; subversion was notably absent. We believe that what we earlier referred to as "revolutionary subversion" should be included in the citizenship rejection criteria.* We would like to make it clear that, with regard to this criterion, the applicant should be judged on his merits rather than being judged by label alone.

22. On the whole, it is the applicant's activity in the years since immigration that is pertinent to the rejection of citizenship on security grounds. There should be, however, as in the present criteria, enough flexibility to permit rejection if the security intelligence agency is concerned that an individual may be lying low, awaiting citizenship before commencing activities that would be detrimental to the security of Canada.

23. Beyond the citizenship security rejection criteria is the R.C.M.P.'s interpretation of the Interdepartmental Committee's guidelines. In our opinion, there are discrepancies between the interpretation and the guidelines — discrepancies which have not been corrected.

24. A series of Security Service misinterpretations of government guidelines is of concern to us. Also of concern to us is the R.C.M.P. description of terrorists as "members or active supporters of. . . guerrilla or liberation organizations". There are many liberation and even guerrilla movements around the world fighting for the same principles of democratic government that we desire to protect in Canada. It has been said that "one man's terrorist is another man's freedom fighter". The objective of the terrorist act must be taken into account by the security intelligence agency; there should be no automatic assumption that an applicant who committed such an act in another country is likely to behave similarly in Canada or even to plan from Canada another act of violent political coercion in his homeland. Reports recommending the rejection of citizenship should reflect such considerations. In future, any interpretation by the security intelligence agency of government guidelines on security screening criteria should be reviewed and approved by the Minister responsible for the agency before distribution to other Ministers or interdepartmental committees.

25. Section 18(1) of the Citizenship Act gives to the Governor in Council discretionary power to refuse citizenship on two grounds — security and public order. There are explicit Cabinet-approved guidelines for security, but none for

[10] S.C. 1977-78, ch.22.

*The Chairman has filed a minority report on this point.

public order. Consideration should be given to what encompasses public order, and rejection guidelines should be drawn up accordingly. Offences against public order in the Criminal Code include such crimes as treason, sedition, sabotage, duelling and piracy. These offences do not include venality of character. In previous legislation "moral turpitude" and a statutory list of other reprehensible behaviour had excluded less desirable immigrants, while "good character" was a statutory requirement for citizenship. These prohibitions were removed when both the Citizenship and Immigration Acts were liberalized in the mid-1970s. The Security Service has continued to provide the Citizenship Registration Branch with reports on reprehensible behaviour. As this sort of behaviour does not meet the security guidelines these individuals are granted citizenship. In future, the security intelligence agency should not be involved in reporting on public order offences or reprehensible behaviour that fall outside its mandate. Information on public order offences not included in the mandate of the security intelligence agency must be obtained from criminal records.

WE RECOMMEND THAT a person be denied citizenship on security grounds only if there are reasonable grounds to believe that he is engaged in, or, after becoming a Canadian citizen, is likely to engage in, any of the following activities:

(a) activities directed to or in support of the commission of acts of espionage or sabotage;

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country;

(d) revolutionary subversion, meaning activities directed towards or intended ultimately to lead to the destruction or overthrow of the liberal democratic system of government;

(152)

WE RECOMMEND THAT any security intelligence agency interpretation of government security screening guidelines be reviewed for approval by the Minister responsible for the agency. Approval to apply the guidelines or to distribute them to other Ministers or interdepartmental committees should not be given until the Minister has satisfied himself that there are no discrepancies between the guidelines and the agency's interpretation.

(153)

WE RECOMMEND THAT guidelines be drawn up and approved by Cabinet interpreting the phrase "contrary to public order" as a ground for the rejection of citizenship; but that the security intelligence agency not be responsible for reporting information concerning threats to public order or reprehensible behaviour unless those threats fall within its statutory mandate.

(154)

D. APPEAL PROCEDURES

26. There is no appeal against a decision to reject an application for citizenship on security grounds. Section 18 of the Citizenship Act states:

> 18. (1) Notwithstanding anything in this Act, a person shall not be granted citizenship under section 5 or subsection 10(1) or be issued a certificate of renunciation under section 8 if the Governor in Council declares that to do so would be prejudicial to the security of Canada or contrary to public order in Canada.
>
> (2) Where a person is the subject of a declaration made under subsection (1), any application that has been made by that person under section 5 or 8 or subsection 10(1) is deemed to be not approved and any appeal made by him under subsection 13(5) is deemed to be dismissed.
>
> (3) A declaration made under subsection (1) ceases to have effect two years after the day on which it was made.
>
> (4) Notwithstanding anything in this or any other Act of Parliament, a declaration by the Governor in Council under subsection (1) is conclusive of the matters stated therein in relation to an application for citizenship or for the issue of a certificate of renunciation.[11]

27. An appeal is allowed to the Federal Court of Appeal against rejections by Citizenship Judges on other grounds. An argument has been made that an appeal against rejection on security grounds is not necessary since rejection is not final but is merely a two-year deferral, and the cost to the individual is only one of delay and inconvenience. Yet, the individual's reputation can be seriously damaged and the delay may be interminable. Moreover, given that the grounds for dismissal may be mere suspicion, it seems only just that a person who has been a resident of Canada for three years should be able to have his case reviewed and tell his side of the story. A Federal Court of Canada decision in 1973 supports this position. The Court ruled that Mr. Tanasic Lazarov's application should be referred back to the Secretary of State for reconsideration and that the applicant was to be given an opportunity to be heard. The fact that a citizenship applicant has no opportunity to dispute the security appraisal was, in the words of Mr. Justice Thurlow, "shocking to one's sense of justice".[12] In the end, Mr. Lazarov reapplied for citizenship, which was granted without a hearing.

28. We agree with the recommendation of the Royal Commission on Security that persons denied citizenship on security grounds should have the right of an independent review. These cases should be heard by the Security Appeals Tribunal we have recommended earlier in this part of the Report. After the Minister has taken the advice of the Interdepartmental Advisory Committee on Citizenship and has recommended rejection of citizenship to the Governor in Council, the applicant for citizenship should be able to request that his case be heard by the Security Appeals Tribunal. The procedure of the Tribunal should be the same as that followed in cases of a denial of security clearance in the Public Service, or for the impending deportation of a permanent resident. The

---

[11] *Ibid.*

[12] *Lazarov* v. *Secretary of State* [1973] F.C.R. 940.

Tribunal should report its findings to the Governor in Council for a final decision. In addition to reviewing cases in which a denial of citizenship for security reasons is proposed, the Tribunal should also review the reports of the security intelligence agency that do not lead to a recommendation of denial. This review procedure, consistent with the Tribunal's review function in other areas of screening, would increase the base of experience of its members, thus enabling the Tribunal to hear citizenship appeals with the benefit of the perceptions gained not only in previous appeals but also from knowledge of cases that did not go to appeal. This review procedure would also provide an independent overview of citizenship security screening procedures.

WE RECOMMEND THAT any applicant recommended for denial of citizenship on security grounds be able to appeal that decision to the Security Appeals Tribunal. The Tribunal should follow the same procedures of appeal and review as for recommended denials of public service and immigration security clearances.

(155)