



SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1985-86

Security Intelligence Review Committee
14th Floor, 365 Laurier Avenue West
Journal Tower (south)
P.O. Box 2430, Station "D"
Ottawa, Ontario
K1P 5W5

(613) 990-8441-- Collect calls are accepted and the switchboard is open from 7:30 a.m.
to 6:00 p.m., Ottawa time.

Minister of Supply and Services Canada 1986
Cat. No. JS 71-1/1986
ISBN 0-662-54510

The Hon. Perrin Beatty, P.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
KIA OA6

June 12, 1986

Dear Mr. Beatty:

Pursuant to section 53 of the Canadian Security Intelligence Service Act, I hereby transmit to you the annual report of the Security Intelligence Review Committee for the fiscal year 1985-86 for submission to Parliament.

Yours sincerely,

Ronald G. Atkey, P.C., Q.C.
Chairman

Jean Jacques Blais, P.C., Q.C.

Frank McGee, P.C.

Saul M. Cherniack, P.C., Q.C.

Paule Gauthier, P.C.

Table of Contents

I. Introduction	1
The Reporting Process	1
Parliament's Watchdog	1
Report Card	4
II. Oversight	11
Establishing Priorities of Review	11
CSIS Resources and Administration	11
Personnel Recruitment, Training and Development	14
Polygraph Examinations	15
Meetings and Inquiries on Specific Incidents	17
Federal Court Warrants	18
Inter-organization Arrangements	20
Ministerial Direction	21
“CIPC”	22
Security Clearances	23
Open Sources	25
Quality of Information on File	26
Annual Reports of the Director and Certificates of the Inspector	
General	27
Future Oversight Research	28
III. Complaints	29
Security Clearances	29
Complaints against CSIS	33
Immigration and Citizenship	34
Human Rights Cases	34
Issues Arising out of Complaints	34
Conclusion	35
IV. Reaching Out and Settling In	37
Parliamentary Liaison	37
Reaching out to Public Servants	37
Briefings and Consultations	38
Foreign Experience	39
Academic Seminar	41
Counsel Seminar	41
Participation in Conferences	42
Committee Personnel	42
Financial Report	42

V. Major Policy Issues	43
Foreign Operations	43
Government Employees, University Campuses	43
Emergency Warrants	44
Other Issues	44

Appendices

A. Research Study on CSIS Recruitment, Training and Development Programs -- Executive Summary	47
B. Ministerial Directives since July 16, 1984	51
C. Summaries of Security Clearance Complaints on which the Committee has Reached Decisions	53
D. Union Representatives at Meetings with the Committee, August and September, 1985	63
E. Text of a Notice Distributed to Public Servants, November, 1985	65
F. Academic Seminar, October 10, 1985	67
G. Legal Counsel Seminar, March 8, 1986	69
H. Security Intelligence Review Committee Staff	71

I. Introduction

The Reporting Process

This is the second annual report of the Security Intelligence Review Committee and the first based on a full 12 month period. The first annual report covered only the four months from our appointment on November 30, 1984, to March 31, 1985. This report deals with our activities in the 12 months ending March 31, 1986.

In preparing this public report, we have had the benefit of the first two annual reports of the Director of the Canadian Security Intelligence Service (CSIS) to the Solicitor General, the first covering the period from July 16 to December 31, 1984, and the second covering the calendar year ending December 31, 1985. Both are substantial documents. The second, much more complete than the first in terms of substantive analysis, was produced in the remarkable time of only two months of the year-end, printed and bilingual.

Besides the two annual reports of CSIS, we received two certificates that the Inspector General, Dr. Richard Gosse, submitted to the Solicitor General. These certificates covered the period July 16 to December 31, 1984, and calendar year 1985, respectively. The certificates are also substantial documents produced with considerable effort and within a tight time frame.

Both the annual report and certificate for 1985 were transmitted to us by the Solicitor General in mid-April, 1986. This allowed six weeks for these important documents to be reviewed and analysed before the deadline for submission of our own annual report to the Solicitor General, in printed and bilingual form, as required by section 53 of the *Canadian Security Intelligence Service Act (the Act)*. While the reporting deadlines adopted by the Service, the Inspector General and ourselves are tight, we believe that they serve a useful public purpose in ensuring that the information, analysis and conclusions in the Committee's annual report -- received eventually by Parliament and the public -- will be reasonably up to date, with a maximum six-month lag between the end of the CSIS reporting period and the tabling of our report in Parliament.

Parliament's Watchdog

In view of recent terrorist activities in Canada and abroad, most Canadians need very little convincing of the need for a modern, effective security intelligence service. Canada had its fair share of tragedy inflicted by terrorists last year, most significantly, perhaps, the Air India disaster in June, 1985. The need to prevent these sorts of incidents simply affirms the importance of the CSIS role in the counter-terrorism field.

But giving support to this type of prevention carries a price -- the potential threat to the rights and liberties of individual Canadians. Parliament was concerned about this when it adopted the *Act*, and it made various provisions to keep this price down. For example, the use of the most intrusive of surveillance techniques (wire-tapping, mail opening and so on) requires a judicial warrant. The Solicitor General may give specific directions to the Director of CSIS regarding the control and management of the Service. An Inspector General is appointed to monitor compliance by the Service with its operational policies and to certify whether the Service has done anything not authorized by the *Act* or the Minister's directions or has engaged in an unreasonable or unnecessary exercise of any of its powers. Finally, Parliament provided for institutionalized accountability through the CSIS annual report, the annual certificate of the Inspector General, and the Committee's annual report, which is submitted to the Solicitor General for tabling in Parliament.

Other than the general accountability of the Solicitor General, the only full Parliamentary review of CSIS (apart from statutory amendment), is through the Committee and its annual report. In some respects, the Committee may be seen as an extension of Parliament. While we are appointed by the Governor in Council and report initially to the Solicitor General, we are appointed "after consultation by the Prime Minister of Canada with the Leader of the Opposition in the House of Commons and the leader in the House of Commons of each party having at least twelve members in that House" (subsection 34(1) of the *Act*). This condition of appointment virtually guarantees our "tri-partisan" nature. Combined with our collective parliamentary, governmental and public service experience and the active role that we continue to play in our communities and professions, it justifies our assuming the role of Parliament's surrogate under the *Act*.

In general terms, our mandate is to see that the Service carries out its work effectively and efficiently -- and within the law. Specific tasks spelled out for us in the *Act* fall into two broad areas:

Oversight.* Subsection 38(a) directs us "to review generally the performance by the Service of its duties and functions", while subsection 38(b) and section 40 permit us "to arrange for reviews to be conducted, or to conduct reviews" with a view to "ensuring that the activities of the Service are carried out in accordance with this *Act*, the regulations and directions issued by the Minister ... and that the activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers". Our work in this area is described in Chapter II.

Complaints. Section 38(c) directs us to investigate complaints that anyone makes about the activities of the Service, complaints about the denial of security clearances in public service employment, in the supply of goods and services to the federal government and in immigration and citizenship matters, as well as to investigate the security aspects of certain complaints lodged with the Canadian Human Rights Commission. In Chapter III, we report on our work in this area.

Chapter IV describes other activities, including communications, liaison and administration, and Chapter V raises certain major policy issues.

In assuming this role as Parliament's watchdog over CSIS, our oversight activities have tended to be event-oriented rather than comprehensive in approach. We have sought to maintain an arm's-length relationship with the Service and other direct participants in the Canadian security intelligence establishment. Granted, we have had to adopt the standard rules and procedures pertaining to any organization operating in this field, such as requiring appropriate security clearances for all our staff and counsel and maintaining the security of sensitive documents. But we have consciously avoided becoming part of the system and giving the appearance of being "insiders"; we are mindful of our role in explaining the system to Parliament and the public without throwing up unnecessarily the smoke screen of "national security" as an excuse for not providing information that can and should be made available in the public interest.

* Oversight is the word used in both the United States and the United Kingdom to mean monitoring and evaluation of security intelligence operations. Because it is a well-established term in the intelligence community, we also use it despite the risk of ambiguity arising from its other meaning as a failure to notice.

Our job has been greatly assisted by our small but hard-working and productive staff. Each staff member brings an important and unique professional contribution to the team, which collectively operates in an efficient and effective manner in conducting research and providing administrative support for us. Like everyone else in government, we and our staff have had to learn to live with budgetary restraint, and this has not been without problems. Our resource problems are far from over, particularly given the increased workload as a result of an important referral from the Solicitor General on bilingualism and personnel management policies and practices. We have received cooperation and support from the Privy Council Office and the Treasury Board in making suitable arrangements for staff and physical facilities for the Committee's operations.

Report Card

The bulk of this report, in describing our activities last year, reflects many of our conclusions regarding the performance by the Service of its duties and functions. However, we thought it might be useful to highlight some of these conclusions in the form of a report card on CSIS and on security clearances by the Department of National Defence. By way of general comment, after 20 months, progress continues to be made in the Service and the future is promising. However, there are still transitional problems.

Operational Activities. To the extent that can be determined through the Office of the Inspector General and independently, the operational activities of CSIS appear to have complied with the law and have not involved an unreasonable or unnecessary exercise by the Service of any of its powers.

Unlawful Conduct. Unlawful conduct by individual members of the Service in 1985 appears to have been restricted, with one exception, to minor parking or traffic violations for which fines were paid in the normal course. The exception involved an incident of personating a peace officer, and, after a report was given by the Director to the Solicitor General, the Attorney General of Canada and to us, it was dealt with internally in a satisfactory manner.

Counter-intelligence and Counter-terrorism Programs. CSIS is operating at a high level of competence and professionalism within its counter-intelligence and counter-terrorism programs, providing useful intelligence assessments and advice to appropriate officials. However, there is still room for improvement even within current budgetary limits, which appear to be a serious constraining force on CSIS operational capabilities.

Targeting Process. The Inspector General found that the CSIS targeting process -- under which individuals and organizations that are or may be conducting activities constituting threats to the security of Canada are investigated -- appears to be functioning well, with due regard to the rights and liberties of those Canadian residents affected. We concur with this finding. In particular, the centralized approval system within CSIS, the various levels of investigation that can be authorized, the length of time of such authorizations, and the nature of information required to be placed before the centralized approving body all leave us and the Inspector General with the general impression that CSIS carries out the targeting process responsibly and well. The Inspector General has suggested some specific improvements, related to the quality and clarity of reports and the role of legal counsel in making targeting decisions. We concur with his suggestions.

Recruitment and Training. The process of recruiting and training new intelligence officers through the Sir William Stephenson Academy at Camp Borden is working well in most respects. This facility will serve CSIS well in the long term.

However, not enough Francophones or women are being recruited, and arrangements for lateral transfers into CSIS of highly qualified people with special skills is lagging. As a result, CSIS in the short term may be simply an extension of the former RCMP Security Service, not the truly civilian body that Parliament intended.

Civilianization. CSIS is unnecessarily defensive and sensitive in discussing civilianization. While we recognize that this process, mandated by Parliament after a lengthy Royal Commission and a full Parliamentary debate, is not without practical problems of transition (e.g., new institutional relationships to be established, phasing out of shared administrative systems with the RCMP), we are disappointed that the progress toward civilianization has been so slow.

We cannot accept the CSIS Director's view that such critical observations somehow reflect unfairly on the professionalism of CSIS employees who came from the RCMP. We have no desire or inclination to denigrate the professional reputations of members of CSIS and the Force from which most of them came. We are the first to recognize their significant contribution to the effective security intelligence programs now in operation. But, also, we now have the advantage of being informed outsiders who, upon being given a fairly substantial look at the inside, have unanimously concluded that Parliament's mandate regarding civilianization is slow to be implemented. We would be remiss in our duty to Parliament if we turned a blind eye to this fact.

We have observed at many levels within CSIS, particularly in senior management, an unwillingness to bring in outsiders. While this attitude may be based on genuine concerns over maintaining security among personnel, it has left the impression that many persons within the organization are still resisting the civilianization process mandated by Parliament.

Concerns have been expressed that because of civilianization and the emphasis put on it, there may be wholesale transfers of senior CSIS personnel back to the RCMP under section 66 of the *Act* (permitted on or before July 16, 1986). But we believe that most CSIS employees regard civilianization as a step in the right direction, with their career opportunities enhanced as a result. This assumes, of course, that there will be adequate financial resources for CSIS to carry out its civilian mandate, an issue which we would hope Treasury Board and the Government do not lose sight of.

Relationship with RCMP. CSIS has made significant progress in clarifying its relationships with law enforcement and other agencies in combatting terrorism. However, it still faces significant impediments to fulfilment of its statutory mandate in this area. We are concerned that, as of the time of writing, CSIS still did not have direct access to the Canadian Police Information Centre (CPIC). We noted in last year's annual report that such access by CSIS officers is essential to their operational capability.

We also have questions about the security intelligence capability of the RCMP, which might operate in parallel with CSIS, duplicating or even conflicting with the Service's primary role mandated by Parliament. As a Committee, we have no oversight powers respecting the RCMP directly, except to the extent that RCMP activities impinge on the performance by CSIS of its duties and functions. Indeed, there is comparatively little independent oversight of the RCMP -- no Inspector General, no Review Committee, no annual report tabled in Parliament, no independent adjudication for members of the public, and less stringent requirements for obtaining warrants authorizing interception of communications. We are encouraged that there is ongoing consultation between the Director of CSIS and the Commissioner of the RCMP regarding investigative responsibilities in counter-terrorism with a view to minimizing overlap and the risk of working at cross-purposes. Suffice it to say at this point that the counter-terrorism roles of CSIS and the RCMP should be complementary, with CSIS primarily engaging in the collection of intelligence and the RCMP in the investigation of security offences and the provision of protective security measures. If CSIS is impaired in the performance of its duties and functions by investigational activities of the RCMP, it should seek direction from the Solicitor General on the matter.

Bilingualism and Personnel Management. As early as the summer of 1985, we began to detect that not all was well in relationships between Québec Regional Command and CSIS National Headquarters. It was not always clear what the nature of the problem was, although it appeared to be a mixture of personality differences, concern over alleged failure of headquarters to implement bilingualism in the Québec region, and differences of opinion concerning RCMP pension rights, bonuses, grievance procedures and promotional opportunities for surveillance officers. The situation erupted into the courts and the press in Montreal in early 1986, and we received numerous complaints under section 41 of the *Act* from individuals, unions and legal representatives.

Given the widespread nature of these problems and their potential for seriously impairing the operational capability of the Service in Québec and the National Capital Region, the Solicitor General on March 19, 1986, asked us to provide him with a special study on the extent to which the reported problems are prevalent in CSIS, with recommendations to remedy any deficiencies which may be discovered. We responded favourably to this request on March 24, 1986, characterizing the Solicitor General's letter and terms of reference as a formal request for a "special report" under section 54 of the *Act*. We were pleased that the Solicitor General had discussed the request with the Director of CSIS, who was fully in support of study and investigation by the Committee.

We expect to report our findings and recommendations to the Solicitor General by the early fall of 1986.

Security Screening. In both our oversight and complaints functions, we have had the advantage of observing closely the work done by CSIS in providing security assessments for other departments and agencies. For the most part we have been impressed with the quality and thoroughness of field investigations and the security screening interviews conducted by the Service. However, there was one complaint before us in which CSIS secretly taped the comments of the public servant being interviewed, a practice which is completely unacceptable and which should cease immediately.

In a review of over 100 files opened since CSIS was created on July 16, 1984, apart from complaints before us, there was not a case where it was found that CSIS exercised "unreasonable" or "unnecessary" powers of investigation or collected information that was unnecessary or excessive.

However, we were disturbed by the time required by CSIS to process requests -- up to nine months, compared with the maximum of three months targeted by the Service at the time of its formation. The facts and figures will be found in Chapter II. While part of this problem may lie with inadequate resources and with government departments that may be requesting clearances that are not really necessary, CSIS must share some of the blame for the backlog and resulting hardship on those present or prospective government employees whose opportunities for advancement are held up while they wait to get the required level of clearance.

The Government's current proposals for changes to the security screening program, about to be implemented as a result of Security Policy Under Review (SPUR), may result in a reduction in the overall number of persons screened for national security purposes. However, there may be offsetting requirements which could demand additional person-years within CSIS. While the SPUR proposals contain major improvements on current policy and should provide better value for money in this important area, we are not at all confident that the overall resource implications for CSIS will be positive. If that is the case, we see no alternative to CSIS allocating a larger portion of its operational program resources to security screening.

DND Security Screening. At the Department of National Defence (DND), security investigations fell far below the CSIS standard. After hearing 16 complaints on denials of clearances by DND, we concluded that many negative security assessments were made as a substitute for personnel management decisions. This is discussed in some detail in Chapter III.

Polygraph Examinations. As discussed in Chapter II, we believe that the "voluntary" polygraph program being implemented among serving CSIS employees should go no further and that polygraph testing of CSIS recruits should cease, at least until a thorough and objective study has been carried out and the Solicitor General and the Government have been able to reach conclusions about whether this technique should be employed by Canadian agencies and, if so, under what circumstances and rules.

CSIS Attitude to the Review Process. If CSIS is still uncomfortable with the process of civilianization, it is even more uncomfortable with the process of independent review. Having a body of outsiders acting as a watchdog is unfamiliar to security intelligence agencies in many countries of the world, including some of Canada's closest allies. Nevertheless, civilian oversight is a growing trend in western democracies as a means of maintaining the delicate balance between the provision of effective security intelligence and protecting the rights and liberties of individual citizens.

Our relationship with CSIS is improving, and we are encouraged by conscious efforts now being made by some within the Service to develop an atmosphere of mutual respect and cooperation as we carry out our respective mandates. Nevertheless, there appears to be a lingering attitude within the Service that the Committee and the Inspector General are a bit of a nuisance, that there is a risk of the review process feeding on itself* and that high-level government discussions should take place on the issue following each reporting cycle**. We believe that this attitude is unwarranted, and we concur with the Inspector General's view that CSIS officials should avoid what might be considered an unwise invitation for political direction as to how statutory responsibilities of review should be carried out. There will be ample opportunity for Parliament to speak when it makes its scheduled review of the legislation three years from now. In the interim, we believe that as we and the Service become more familiar with each other's roles and responsibilities, relationships will develop which should prove to be mutually beneficial.

For members of the Service, exposure to the new and challenging reality of oversight and accountability to Parliament should be a positive experience. For us, the appropriate line between review functions carried on in a creative and constructive atmosphere and interference in the day-to-day operations and management of the Service should become clearer. In this respect, we wish to state categorically that we recognize the exclusive role of senior management and the Director of CSIS in the day-to-day operations and management of the Service.

What should emerge in the end is the sort of healthy and creative tension between two bodies that is based on mutual respect and a commitment to excellence in carrying out their respective statutory mandates in this most delicate of areas.

* a comment in the 1985 Annual Report of the Director of CSIS

** ibid

II. Oversight

Establishing Priorities of Review

In last year's annual report we characterized our approach as "a genuine curiosity sprinkled with a healthy dose of skepticism -- factors which are an important part of the Canadian parliamentary tradition". In the year ending March 31, 1986, we focused on a number of areas:

- the CSIS budget (multi-year operational plan);
- recruitment, training and development at CSIS;
- use of the polygraph ("lie detector");
- various acts or threatened acts of terrorism in Canada;
- judicial warrants;
- CSIS arrangements with the RCMP and other bodies;
- ministerial directions to CSIS;
- security screening;
- CSIS use of open sources;
- counter-subversion operations and the problem of unwitting participants; and
- collection of information by CSIS and file retention (accidental by-products).

This report deals with many of them.

CSIS Resources and Administration

Mandate. One of our tasks under the *Act* is to "review generally the performance by the Service of its duties and functions". We thus examined the CSIS budget, to see whether the Service had adequate resources to carry out its work, as well as certain elements of its administration.

Transition. Before CSIS was created in 1984, its work was the responsibility of the RCMP, which provided accommodations and such central services as financial administration. CSIS has had to establish facilities and services of its own. In some areas, RCMP systems have had to be tailored to the needs of a smaller organization.

CSIS is having to develop its own services in a climate of severe restraint. The new agency also faces extensive demands for information from oversight bodies -- something the RCMP Security Service did not have to deal with. In 1985-86, for example, we made 70 written inquiries and received oral briefings on a wide variety of topics.

While all areas of government must share the burden of restraint, we are concerned that CSIS may be faced with a very serious resource squeeze.

Accommodations. CSIS has a multi-year capital plan to build and equip facilities separate from those of the RCMP in a number of Canadian cities. In Ottawa, a new national headquarters is planned. However, there have been serious delays.

The Service has provided us with a copy of a special audit concerning the renovation of a building in Montreal to serve as regional headquarters for Québec. This audit was carried out by the Auditor General at the request of a former Solicitor General. The report indicates that this project could be delayed by as much as three years, and that the real cost may consequently be higher than planned. While the report acknowledges that some of the delays were beyond the control of the Service or were to be expected in any new venture, it also noted that CSIS:

- did not examine the cost efficiencies of various sites in its initial search for a location;
- has weaknesses in project management, notably a lack of clearly defined responsibilities; and
- was unable to meet certain milestone dates and made late amendments to the specifications.

We will continue to monitor the completion of capital projects and to inquire into the changes made by CSIS in response to the Auditor General's report.

PEMS. At present, all government departments and many agencies have an annual planning cycle based on the Policy and Expenditure Management System (PEMS). The Service has started putting PEMS in place, but it is not as yet fully implemented.

Examining the Service's PEMS documentation in light of Treasury Board guidelines and discussing implementation with CSIS officials, we noted some difficulties. The documentation includes non-measurable objectives, which are not compatible with the intent of PEMS. In any event, follow-up "statements of results" are generally lacking, so that the degree to which objectives were achieved is not apparent from a reading of the documentation. These deficiencies impede systematic budget analysis.

We appreciate the problems associated with measuring the results of security expenditures. We also recognize that few departments or agencies fully adhere to PEMS documentation guidelines. We do feel, however, that knowledge of how resources are transformed into end results is of more than academic interest. In times of restraint, the Government must be fully aware of the implications of reductions, and the Service must be able to state the results of security expenditures clearly so it can compete for scarce resources.

Bilingualism and Personnel Management. At the request of the Solicitor General on March 19, 1986, we have undertaken a special study on problems of bilingualism and personnel management policies and practices, reported from the Montreal office of the Service as described in the introduction to this report.

In early April, we commenced our investigation of this situation with the assistance of Pierre Gagnon, a Quebec City lawyer with considerable experience in labour-management issues, and the Office of the Inspector General. Discussions were held with the Office of the Commissioner of Official Languages with a view to co-ordinating his and our investigations of the implementation of Canada's official languages policy within CSIS and to avoid duplication, overlap and unnecessary expense.

Our immediate task has been to focus on the extent, if any, to which the operational effectiveness of CSIS has been impaired by:

- failure to observe the Government's official languages policies in the Québec and National Capital Regions;
- ineffective, poorly executed, inappropriate or misunderstood personnel policies and practices, with particular reference to the Québec and National Capital Regions;
- inappropriate or misunderstood pay and benefits policies, with particular reference to the effect of such policies in the Québec and National Capital Regions; and
- ineffective, poorly executed or misunderstood promotion and grievance procedures, with particular reference to the effect of such policies in the Québec and National Capital Regions.

We expect to report our findings and recommendations to the Solicitor General by the early fall of 1986.

On his own initiative, the Inspector General in early 1986 reviewed the use of Canada's official languages in obtaining warrants under the *Act* in the Québec Region during 1985. This review was undertaken to determine whether undue delays were caused though lack of bilingual capacity at CSIS headquarters. He concluded, after examining relevant files and records, that warrants were not delayed for this reason, although there were delays in translating certain documents after the warrants were issued. The perceived problems in Québec relating to warrants appear to have arisen through the failure of some personnel in Montreal to understand the elaborate process necessary under section 21 of the *Act* for obtaining warrants and insufficient communication between CSIS headquarters and Montreal to explain non-linguistic problems associated with preparing warrant applications to the court. We are advised that these communication and information problems are currently being resolved.

Personnel Recruitment, Training and Development

In last year's annual report, we indicated that examination of CSIS training and development would be a priority. After a briefing from the Service, we launched a full research study, which was completed in March, 1986, and forwarded to the Solicitor General, the Director of CSIS, and the Inspector General.

We recognize that CSIS management has overcome many obstacles and achieved good results in a number of areas. Particularly impressive was the speed with which the Service created from scratch a training program that got a very high rating from its first class of recruits. And it is only fair to note that some strains will exist in any transition process -- are, indeed, unavoidable in a career service with a competition system for transfers and promotions.

We recommended that:

- CSIS recruit additional personnel from outside the Service to middle-management positions;
- CSIS advertise openly and widely for recruits;
- the recruitment pool be widened to encourage greater participation by Francophones and women in the operational and intelligence officer categories. We also suggested more recruitment of individuals with foreign-language skills;
- CSIS management intensify current efforts, with the Public Service Commission, to keep unionized employees from losing the right to compete for other public service jobs as a consequence of CSIS' designation as a separate employer;

- more Francophones be hired at senior levels, that all communication with Québec and all documentation for national use be made available in French, and that senior management recognize and make a commitment to solving the bilingualism issue;
- efforts be made to develop additional internal training programs and tradecraft courses for employees;
- an employee assistance program be established to deal with personal and work-related problems, and that it operate on a basis of strict confidentiality; and
- greater efforts be made to improve communication between senior management and employees.

An executive summary of our findings and conclusions can be found in Appendix A.

Polygraph Examinations

We have grave doubts about the present use of the polygraph -- better known to the public as the "lie detector" -- by the Service for employment and security clearance screening. Taking a polygraph examination is a condition of employment for recruits, and current employees have been asked to "volunteer" for examinations. Questions relating to both lifestyle and loyalty are posed to recruits in these examinations. Current employees are asked questions related to loyalty only, not lifestyle.

In polygraph examinations, certain physiological reactions of subjects are monitored while they respond Yes and No to questions. Quickened pulse and breathing, for example, in response to particular questions, may be read as signs that the subject is deceptive.

A distinction has to be drawn in the use of the polygraph between criminal investigation, on the one hand, and employment and security clearance screening, on the other. There is some evidence that polygraph examinations can be a useful tool in criminal investigation. But there are no generally accepted scientific studies that establish their validity in employment and security clearance screening, and it is this use we are discussing here. Supporters generally cite anecdotal rather than scientific evidence in favour of the polygraph in security clearance screening.

Nonetheless, there are some who argue that, used as one indicator among others, the polygraph is an invaluable guide to the honesty of individuals tested. But others point out that it can wrongly point the finger of suspicion and put an intolerable onus on those who fail to prove their honesty.

The Service must, of course, guard against penetration by those who would betray Canada for ideology, personal gain or other reasons. We know that the use of polygraph examinations is widely accepted in the U.S. intelligence community to screen recruits and employees, although not without objections from some prominent Americans.

The Canadian Security and Intelligence Service is trying to be responsible in this area. CSIS examinations are performed by trained psychologists.* And the Service says that "normally" no one is denied security clearance or employment solely on the basis of a polygraph examination; supporting evidence from other sources is required.

But we are not satisfied with these safeguards. The accuracy of polygraph results lies at the heart of the issue. Assuming that the examinations were 90 per cent accurate -- a higher estimate than most experts claim and that one out of every 1,000 persons tested were disloyal, then in a sample of 1,000 candidates, 100 innocent people would be labelled dishonest and the one truly dishonest person would have one chance in 10 of not being caught. Thus, there is not only the risk of grievous injustice to honest and loyal Canadians, the polygraph is not even an airtight bulwark against penetration of the Service by disloyal and dishonest people.

Most importantly, we do not think that CSIS can sustain in day-to-day work its policy against making polygraph results the sole determinant of security clearances and employment --- even "normally". Negative results on a polygraph examination would be taken so seriously by so many people that injustices could not be avoided. Indeed, in one complaint before us in 1985, overwhelming reliance on the polygraph was clear, although it was denied with palpable sincerity by those whose judgement the polygraph readings had so obviously swayed.

* We also wish to record that we were disturbed to find that the Service did not have on call a trained psychologist who could administer the examinations in French. This failing has been corrected as of February, 1986.

In a similar vein, we do not believe that the examination of current employees can be truly "voluntary". Anyone who showed any reluctance would clearly be suspected of having something to hide, with the result that pressure to be examined would almost certainly be irresistible for all but the bravest souls.

Finally, we are also concerned that as the polygraph becomes routine for members of the Service themselves, its use will spread unnecessarily throughout the government.

For all of these reasons, we urge that the use of polygraph examinations for employment and security clearance screening stop, at least until a thorough and objective study has been carried out and the Solicitor General and the Government have been able to reach conclusions about whether the use of such methods is compatible with the values of a free and democratic society.

Meetings and Inquiries on Specific Incidents

We actively question the Service on incidents and actions of national import, both on our own initiative and following inquiries from the public. We wish to record our appreciation of the Service's general candour in these matters. Overall, we believe that CSIS took appropriate and adequate action.

Air India and Narita Airport Disasters. On June 23, 1985, Air India flight 181/182 crashed into the Atlantic Ocean off the coast of Ireland. On the same day, there was an explosion in luggage unloaded from CP Air flight 003 at Narita Airport in Japan. The cause of these incidents has not been officially determined, however bombs planted by terrorists are strongly suspected. We were concerned with the intelligence produced in this matter and the quality of airport security in general, and we started questioning CSIS officials on these and related issues. We intend to pursue this matter with vigour but not in a way that will interfere with ongoing CSIS and RCMP operations.

Airport Hoax. In December, 1985, the RCMP was informed of an alleged Libyan plot to place an explosive device on a commercial passenger flight originating from Ottawa. Security precautions at several airports were subsequently increased, at significant expense to Canadian taxpayers and inconvenience to travellers. The RCMP ultimately determined, with CSIS assistance, that the alleged plot was a hoax. We questioned CSIS officials on the incident and on airport security in general.

Expulsion of Bulgarian Diplomat. On July 22, 1985, following a CSIS investigation, the Department of External Affairs declared a Bulgarian diplomat, Vitaly Ivan Delibaltov, *persona non grata*. Information provided by CSIS had indicated that Delibaltov was involved in collecting unauthorized information, an activity incompatible with his diplomatic status. Our interest arose from media discussions and comments on this case.

Deportation of Taiwanese Official. In January, 1986, Patrick Chang, president of the Canada-Taiwan Chamber of Commerce, received a deportation order, and in March, 1986, abandoning court appeals, he returned to Taiwan. According to media reports, some members of the Chinese Canadian community believed that the government decision was racist and that Chang had no opportunity to defend himself. We have asked to be informed of the specific reasons for this deportation decision.

Federal Court Warrants

Mandate. The Service may, with the approval of the Solicitor General, seek warrants from the Federal Court of Canada for such purposes as planting electronic listening devices, conducting clandestine searches or opening mail.

The *Act* does not assign to us any specific responsibilities regarding warrants. However, we have a general duty to flag unreasonable or unnecessary use by the Service of its powers. And we are also directed by the *Act* "to compile and analyse statistics on the operational activities of the Service". This responsibility permits us to fill a gap in reporting on warrants. Before the *Act* was adopted, the Solicitor General published certain statistics under the *Official Secrets Act* on the use of warrants in security matters. This portion of the *Official Secrets Act* was repealed when the *Act* was adopted, so the Solicitor General no longer has this duty. With his concurrence, we have decided to report to Parliament on the use of warrants.

Statistics. Statistics found in Table 1, provided by CSIS, cover the calendar year 1985. Section 21 of the *Act* provides for new warrants and section 22 for the renewal of existing warrants.

Activities authorized by these warrants included wiretapping, eavesdropping by microphone, capturing of optical images, interception of recorded communications, searches for documentation and paraphernalia and the interception of mail.

In 1983, the last full year in which warrants were issued under the *Official Secrets Act*, the Solicitor General approved 525 warrants. The average length of time a warrant remained in force was 253 days.

Table 1. Warrants Granted to CSIS, 1985

New warrants issued under Section 21	82
Warrants renewed under Section 22	27
Average length of time for which warrants were in force:	173.58 days

However, a direct comparison of the numbers of warrants issued under the two statutes is not possible because of differences between them. Under the *Official Secrets Act*, in general, each warrant authorized the use of only one covert technique, such as a wiretap, against only one "target". Thus the warrant statistics provided to Parliament under that *Act* clearly showed the extent to which such powers were used. Under the new *Act*, however, one warrant can authorize the use of many devices against many targets.

Thus, statistics on warrants issued under the new *Act* convey substantially less information than those compiled under the *Official Secrets Act* about the extent of authorization of highly intrusive devices. We are negotiating with CSIS a more informative arrangement of statistics to present to Parliament in future. In the meantime, we have examined recent trends and believe that there has been no increase in the use of intrusive investigation techniques authorized by warrants over the last three years. Differences in the average length of time warrants are in force may be explained by provisions in the new *Act* for 60-day warrants and by the change-over to a new warrant approval system.

Observations. We were briefed by CSIS on the use of warrants generally, we read the affidavits sworn by CSIS officers in support of requests for particular warrants, we read the specific terms of the warrants issued by the Federal Court, we reviewed the quarterly reports on outstanding warrants, and we undertook some statistical analysis. No improper use of warrants or the warrant application procedure was noted.

Future Review. The public presentation of warrant statistics in any detail could jeopardize security intelligence operations. We plan, however, to examine this process in some depth, with the intention of ensuring that there is no unnecessary or excessive use of the Service's powers. We also intend to go behind the affidavits to examine the files which support them. We will question the Service on significant variations in the use of intrusive techniques, and, if need be, report to Parliament on these changes.

Inter-organization Arrangements

Mandate. The *Act* directs us to review arrangements that the Service enters into with federal departments, provincial authorities and police forces, and foreign governments and institutions. Under such arrangements, the Service may conduct security clearance investigations for other agencies. It can also make arrangements for such purposes as sharing information and conducting joint operations.

Access to Data Bases. We have received copies of two memoranda of understanding that give the Service access to Canada Post and External Affairs data bases. Under these agreements, CSIS can request information under paragraph 8(2)(e) of the *Privacy Act* -- information required to enforce any law or carry out lawful investigation. We have examined the two agreements and believe that both fall within the letter and spirit of the *Act*; they involve no undue encroachment on individual privacy or liberty.

CSIS has advised us that four further memoranda of understanding giving it access to federal data banks have been finalized. Negotiations are underway with a view to gaining access to a number of other data banks held by federal departments and by certain provincial authorities. We will review these agreements when they are signed and copies are received.

Foreign Arrangements. We have been briefed on arrangements that the Service has with friendly powers. These fall into three categories. There are formal agreements in which the terms are explicitly documented and there are exchanges of notes, including an exchange between the Canadian embassy and the foreign ministry of the country concerned. Second, there are informal arrangements in which a general understanding of co-operation is exchanged between services or at the embassy level. Finally, there are ad hoc arrangements in which liaison officers reach a verbal understanding.

CSIS provided us with copies of such agreements that it inherited from the Security Service of the RCMP -- thousands of pages, which we perused. Questions arose and, in most cases, clarification has been received.

However, we believe that these arrangements should all be reviewed in light of the new *Act* and renegotiated. We made the same recommendation in last year's annual report. CSIS' lack of action to date suggests that it does not agree.

U.S. Immigration and Naturalization Service. We inquired into the provision of information by the Canadian government to the United States Immigration and Naturalization Service (USINS) and found that before 1980, the RCMP Security Service provided USINS with information that may, in some cases, have been used to place individuals on a USINS "Lookout List" which is kept at border crossings. This is a list of individuals to be refused admission into the United States. The Canadian government cancelled this agreement in 1980 and asked the U.S. government to purge from USINS files all information previously provided.

We are concerned that USINS has been unable to comply with this request, offering various legal and administrative reasons. But it has agreed to review files on a case-by-case basis. That is, when Canadian authorities ask that Canadian-supplied information on a given individual be removed from the file, USINS will review the case and may comply. Exceptions occur when USINS has similar information from other sources.

Canadians who are on the "Lookout List" because of information supplied by Canadian authorities before 1980 can apply to CSIS to ask USINS to have the information withdrawn. If they are not satisfied that CSIS made such a request, they can lodge a complaint with us.

Ministerial Direction

Mandate. The *Act* provides that when the Solicitor General issues written directions to the Service, we must be given copies.

Past Solicitors General have provided direction to the Service in two forms -- directives and direction. Ministerial directives are formal instructions covering a certain type of operation. They normally require that certain matters be referred to the Solicitor General for decision. Ministerial direction normally takes the form of correspondence on specific cases in which the Solicitor General incidentally provides policy guidance with respect to fairly narrow categories of cases.

Review. We received from the Service a "Compendium of Ministerial Direction" containing all known written directives and direction. We have reviewed this document, and asked a number of questions on specific items. We understand that all Ministerial directives are currently being revised to conform to the new *Act*, and we will continue to monitor the situation.

Fourteen new directives have been issued since CSIS was established. They are listed in Appendix B.

“CPIC”

We are disturbed by the fact that CSIS still does not have full, direct access to Canadian Police Information Centre (CPIC) data banks, which let users find out instantly about such things as vehicle registration and criminal records.

This was an issue we raised in last year's annual report. Because we believe that CSIS officers need direct access to CPIC to work effectively, we said then that the Canadian Police Information Centre Advisory Committee should allow such access. The RCMP is a major participant in this committee.

In February, 1986, we asked for a progress report and learned that, pending further discussions, the Service is still denied direct access to a major portion of CPIC information. To get this information, CSIS must apply to the RCMP. Even for the files to which access was granted, the Service is still waiting for the RCMP to supply the necessary computer terminals and software.

We have strongly urged the parties involved to resolve their difficulties and have suggested to the Solicitor General that he consider intervening personally, as both the RCMP and CSIS report to him.

As noted in the introduction, we have no oversight powers respecting the RCMP directly, except to the extent that RCMP activities impinge on the performance by CSIS of its duties and functions. On July 29, 1984, just after the *Act* came into force, the then Solicitor General issued guidelines of the principles on which the security responsibilities of the RCMP and CSIS should be based. To the extent that these guidelines result in both organizations working at cross-purposes, particularly in the field of counter-terrorism, they should be re-examined by the Solicitor General with a view to clarification. We wish to state our position clearly: the roles of CSIS and the RCMP should be complementary, with CSIS engaging in the collection of intelligence and the RCMP in the investigation of security offences and taking responsibility for protective security measures.

Security Clearances

In October, we asked the Inspector General to review the Service's investigative role when security clearances are requested by government departments. One of many reasons for the request was delays in clearing our own staff to the Top Secret level. Investigations of employees who had already been working in the government were taking more than six months.

Our preliminary survey of all federal departments showed that this was not unusual. On average, it takes six to seven months to complete a Top Secret security clearance investigation, and it can take up to nine months. There was evidence that departments were losing potential employees because of the length of time it takes to obtain clearances.

It should be noted, however, that it takes considerably less time for Confidential and Secret clearances, as they do not require field investigation. The normal waiting period at the Confidential and Secret levels is from six to eight weeks.

We asked the Inspector General to review the following specific matters:

- the role played by the Service in the security clearance process;
- the workload imposed upon the Service by departments and agencies;
- arrangements between the Service and federal, provincial and foreign agencies in this area and, in particular, the nature of information exchanged;
- criteria used by the Service to measure an individual's suitability for each level of security clearance and, in particular, the use of Cabinet Directive 35 as a standard; and
- relevant ministerial directives.

Since CSIS also advises the government about landed immigrants and potential immigrants, we asked the Inspector General to review CSIS' role in citizenship and immigration cases.

Data. The Service received 69,647 requests in 1985 for security assessment related to Public Service employment. More than two-thirds 48,000 -- were for Secret and Confidential clearances, while the remaining 14,647 were for Top Secret clearances. Of the total number of requests, 4,438 were for a full field investigation on applicants or employees of the Public Service and 2,898 of these were completed and a security assessment report submitted to the departments concerned.

The reported average cost of a Top Secret clearance was \$1,425 and of a Confidential or Secret clearance \$13.62 (exclusive of a criminal records check). We were surprised at how low these figures are. We suspect that they include only direct costs and exclude the share of overhead that could be attributed to each investigation.

Backlog. Both the CSIS headquarters and the regions have a backlog of security screening applications. The study attributes this to a number of reasons, as follows:

- a quarter of the positions in the Security Screening Branch have not yet been filled;
- new staff in this Branch has not yet reached peak efficiency;

- there has been a substantial increase in requests for time-consuming Top Secret clearances. This was explained in part by the change of Government, which brought a surge of requests for clearance of new staff in ministers' offices; and
- there are delays in criminal records checks related to delays the Service has faced in getting direct access to the Canadian Police Information Centre (CPIC), as discussed earlier in this chapter.

The study reported that there are about 4,000 applications at all levels at some point in the system. We were disturbed to learn that about a thousand cases are delayed because the files are "in typing" (i.e., the assessments have been written and sent to the typing pool). There were 700 such files in National Headquarters in February and March, 1986, and almost half that number again at the Ottawa Regional Office. Meanwhile, about 280 new requests are coming in daily.

Recommendations. The study made a number of recommendations for improving the security clearance process. We will review them in conjunction with new policies and operational guidelines on the security classification and personnel screening system, which the Government is expected to issue shortly. These policies and guidelines will replace Cabinet Directive 35, which has set criteria and procedures for security clearances since 1963. They are intended to establish a security screening process that meets the requirements of departments within the letter and the spirit of the *Act*.

We will monitor these policies, together with related guidelines issued by Treasury Board, to assess their impact on the security screening process and on the Service.

Open Sources

Among shortcomings that the McDonald Commission found in the RCMP Security Service was an almost complete reliance on information from covert sources. The Commission stressed the value of organizing and developing a mechanism for collecting information from public sources as an alternative to such intrusive activities as wiretaps and infiltration. Major open sources include scholarly periodicals and the mass media.

Created as a result of the McDonald Commission findings, CSIS has taken some first steps toward the use of open sources. With advice from the Centre for Conflict Study at the University of New Brunswick, it has established an Open Sources Research Unit with two components -- the existing library and a new team charged with compiling and distributing open-source information to operational desks.

Assessment. The Service is moving in the right direction but we would like to see it move further and faster. The open sources unit is still not fully operational, as some staff positions remain vacant; the library continues to grow, but modestly.

Staffing of the research component is also a concern. The Service has preferred "street-wise" intelligence officers rather than individuals with broad academic or analytic capability and knowledge of government. In operations, the value of street-wise intelligence officers is beyond dispute. But we feel that experienced, university-trained professionals might be more appropriate for positions in the research unit.

In addition, we have not seen evidence to convince us that making open information more widely available within CSIS has been reflected in wider use of this information by intelligence officers in the field. A change in attitude may be as important as increased resources.

A somewhat similar concern was expressed by the Inspector General in his certificate, in the following terms:

... What has surprised me is that some of the [External Affairs Department] specialists have had little or no contact with the analysts in the CSIS that have responsibilities for these activities. I know, of course, that the CSIS and External Affairs have formal links and that, in that context, discussions take place in all areas of mutual concern, but it struck me that both CSIS analysts and External Affairs officials have much to gain from a greater direct interchange of information and views. It seems to me that interchange should be developed and encouraged. From the point of view of the CSIS, I am certain that it would enhance the quality of their analysis, in some areas at least. I am sure External Affairs would benefit as well, and the impression I had was that such interchanges would be welcomed.

Quality of Information on File

We have asked CSIS for reports on two potential problems with the information in its files on individuals and organizations.

First is the possibility that some information in files inherited from the RCMP Security Service is out of date or does not satisfy the definition that the *Act* gives to the term "threat to the security of Canada". This definition includes, of course, such things as espionage, sabotage and violence in the pursuit of political goals, but it explicitly excludes "lawful advocacy, protest or dissent". By implication it excludes personal information unrelated to security concerns. We have asked CSIS what action has been taken to purge Security Service files of any inappropriate information they may contain.

Second, in its own work, CSIS may itself sometimes get "accidental by-products" -- that is, information that does not meet the *Act's* definition of a threat but which can be useful in some way to public administration. Of course, when an investigation turns up evidence of crime, the police must be told. Otherwise, such information is to be discarded. We have asked for a full accounting of the measures put in place to ensure that this happens, so that we can assess their adequacy.

When these two reports are received, they will be compared with the elaborate procedures proposed by the McDonald Commission for keeping non-security information out of security files.

Annual Reports of the Director and Certificates of the Inspector General

Mandate. The *Act* makes extensive provisions for review of the annual report that the Director of CSIS submits to the Solicitor General on operational activities. First the Inspector General examines the report and issues a certificate indicating whether he is satisfied with it, whether the Solicitor General's directions have been followed and whether the Service has used its powers reasonably and only as necessary. Then, both the annual report and the certificate come to us for review.

1984. In our previous annual report, we could not comment on the 1984 report of the Director or the certificate of the Inspector General as they were not available soon enough. Thus they are dealt with in this report.

Like the Inspector General, we noted that the 1984 Director's report contained much useful background but that it was short of facts and figures. Along with the Inspector General and the Deputy Solicitor General, we took part in a meeting, held in November, 1985, with the Service to develop a format for future annual reports.

We noted the Inspector General's comment that his certificate was "limited in scope" as staff shortages prevented extensive audits of operational activities to ensure compliance with the *Act* and with the Solicitor General's directions.

1985. Incorporating many of the suggestions made by us and by others, the Director's 1985 report was far more useful than the 1984 report. It describes CSIS operational activities and certain targets of surveillance in some detail. We were also pleased to note that the report came out in good time. Like the Inspector General, we were generally satisfied, but we would still like to see the inclusion of more facts and figures on such matters as the precise breakdown of the budget among various activities.

After a careful reading of the report and accompanying certificate, we support the Inspector General's statement that he "was generally satisfied that the investigative authorization process was being carried out reasonably and well". We note, however, that once again the Inspector General felt he could not certify compliance with the *Act* or with directions from the Solicitor General because staff shortages prevented thorough audits.

Usefulness of the Annual Report in Oversight. It has become apparent that the annual report of the Director will not be a major source of information in the oversight process. A similar conclusion has been reached by the Inspector General. As he says in his 1985 certificate: "Even if it did contain a mass of information about the CSIS's operational activities, it would be necessary to go behind the report and examine files and conduct interviews in appropriate cases".

Most of the information in the report will already be known to us if we have carried out the review function properly. We expect that we will rely mainly on our own research and information supplied in confidence by the Service to carry out our oversight tasks.

Nevertheless, the annual report will certainly often stimulate the initiation of particular inquiries and will be generally useful to us. In addition, we will often wish to request additional evidence to buttress conclusions reached.

Future Oversight Research

We have identified a number of major initiatives to be pursued during the period remaining in our five-year term. In the coming year, we hope to examine the following subjects:

- federal court warrants -- (a) whether activities authorized by warrant are generally effective in producing needed information; and (b) close study of warrants issued to ensure there is no unreasonable or unnecessary use of the Service's powers;
- agreements with other bodies for the exchange of information;
- Solicitor General's directives -- what they say and how systematically they are applied;
- human sources -- an analysis and review of the product gained and its overall reliability;
- counter-subversion -- the activities of the Service in this area and a review of the product gained; how it is used by those who get it and its usefulness;
- "accidental by-products" -- how the Service deals with non-security information about individuals and organizations that comes its way in the course of its work;
- bilingualism and personnel management policies and practices at CSIS;
- use of security intelligence product -- who are the legitimate consumers?; and
- mail opening.

We also intend in the coming year to begin a regular and systematic review of operational statistics. To date, we have asked for and received statistics on various operational activities, including the use of intrusive powers and the allocation of operational resources. Actual compilation and analysis of the information provided has, however, been delayed pending acquisition of appropriate computer capacity.

III. Complaints

We received many more complaints than we had expected -- more than 600 in all. However, fewer than 100 raised strictly security issues; the overwhelming majority were made against the Service's practices regarding use of French and English.

Apart from that, the denial of security clearances prompted the most complaints -- 81. We attribute this in part to our own efforts to inform Canadians of rights that Parliament has given them. But it is clear that mandatory notification of those whose security clearances are denied was the major factor. In this respect, the *Act* is doing what Parliament intended it to do.

We have some concerns that "security" is sometimes being given too broad a reading, especially by the Department of National Defence (DND). Some gaps that Parliament may not have meant to leave open were also detected in the *Act*. These concerns will be made clear later in this chapter.

Security Clearances

Mandates. Under the *Act*, complaints can be made to the Committee by: a person refused federal employment solely because a security clearance has been denied; a federal employee who is dismissed, demoted or transferred or denied a promotion or transfer for the same reason; and anyone refused a contract to supply goods and services to the government for the same reason.

In all of these cases, persons denied a security clearance must be notified and told that they may lodge formal complaints with us. After investigation and *in camera* hearings, Committee members report their findings and any recommendations to the Solicitor General, the Director of CSIS, the deputy head concerned, and the complainant.

Investigations and Recommendations.

Hearings have been completed and recommendations made in 21 security clearance cases. While this accounts for only about a quarter of the complaints received, 44 complaints originating in DND are being reconsidered by departmental officials and 14 were withdrawn (nine because they fell outside our jurisdiction and five because they were resolved without formal hearings). Thus, only two complaints were under active consideration at year-end -- although, of course, the 44 being reconsidered by DND are still active Committee files.

The outcomes of the 21 cases in which we reported findings and recommendations during the year are as follows:

- In eight, we supported the denial of a security clearance. However, in five of these cases, we recommended that the security status of the individual concerned be reviewed earlier than planned, and these recommendations were all accepted.

- In 12 cases, we recommended that the denial be overturned and the security clearance granted or restored. In one case, from the Department of Agriculture, our recommendation was still under consideration by the Deputy Minister at year-end. In the other 11, all from DND, the Chief of the Defence Staff accepted five recommendations, ordered further investigation in four cases, directed in one case that the complainant be reconsidered for a Top Secret clearance at some time in the future, and rejected one outright. In this last case, the complainant may be taking legal action against the Department directly, although it is possible that the matter could be resolved through negotiation.
- In one case, we recommended that the matter be placed before the Public Service Staff Relations Board as national security was not the real issue.

A brief summary of each case dealt with by the Committee can be found in Appendix C.

Quality of Security Investigations.

We indicated earlier in this report that security screening by CSIS was almost always fair and thorough, if too slow. A notable exception found was a case where the subject being interviewed by CSIS (the public servant whose security clearance was in issue) had his comments during the interview secretly taped by CSIS. While such taping is not illegal where one party (the CSIS interviewer) consents, it is a completely unacceptable practice that assaults the privacy of the individual being interviewed, and should cease immediately.

But problems were endemic in screening by the Department of National Defence. At DND, clearances were commonly denied on the strength of rumor and second- or third-hand hearsay that was not always verified. DND appeared to be hypnotically concerned with pre-service and early service minor offences despite the clearest possible evidence that the individuals concerned had reorganized their lives and had demonstrated their positive potential and value to the Forces. This is particularly puzzling because in most of the cases we dealt with, it was clear that the environment within the Forces helped these young people reorganize their lives. Most serious and most common of the problems we saw was a tendency to draw adverse inferences and conclusions from inadequate evidence. Also, some investigations clearly lacked objectivity: adverse information was accepted at face value while favourable evidence was discounted.

In the 44 cases now being reconsidered by DND, the original investigation failed to respect safeguards specified in Cabinet Directive 35. For example, none of the complainants had been given a chance to meet with a senior officer so they could try to resolve doubts about their reliability. Indeed, most had not been interviewed by even the investigating officer, so they were not aware of these doubts until after they were notified that a security clearance had been denied. At our request, DND agreed in January, 1986, to reconsider these cases, following procedures set out in Cabinet Directive 35.

However, this was not the only concern we felt about arrangements for security clearances at DND. Our examination of complaints originating there suggested that not enough care was being taken to distinguish between threats to national security and personnel problems. In many cases, the activities or attitudes for which security clearances were denied are not within the ambit of either the *Act* or Cabinet Directive 35. It is not for us to advise the Department on suitable counselling, disciplinary or other personnel management procedures. But we do not hesitate to say that many of these cases should not have reached us as national security matters. This was particularly so when occasional use of soft drugs was the principal issue.

As part of our discussions with DND on these issues, we asked for and obtained a briefing on its concerns about drug use. The briefing team was led by the Assistant Deputy Minister (Personnel), Lt.-Gen. Paul Manson. While we understand the need for strict standards concerning even the minor use of drugs in the Forces, we do not believe that the security clearance process should be used as a weapon in the battle against drug use.

DND's special sensitivity to security concerns goes some way to explaining the fact that it was the source of more than three-quarters of the complaints we received about security clearances - 67 out of 81. But overuse of the security process to deal with unrelated matters is also, in our view, a significant factor.

Response to Committee Recommendations. We are concerned, too, by the high proportion of our recommendations rejected by the Chief of the Defence Staff, though the number of cases involved is small, and it may be too early to draw definitive conclusions. We are especially troubled by DND decisions to re-investigate cases after Committee hearings and recommendations.

In the *Act*, Parliament clearly left the final decision in security clearances to deputy heads, but it is not plausible that it intended review by the Committee to be merely a detour. We follow court-like rules in which all parties can be represented by expert counsel, call witnesses who testify under oath and cross-examine witnesses called by other parties. Only then do we make a report with our findings and recommendations.

Further security inquiries by a department should be unnecessary following such hearings, unless there are new circumstances or facts that did not exist or were not known at the time of our hearing. We are disturbed that individuals who use rights of appeal granted to them by Parliament and attend hearings where DND has every opportunity to question them should then be the subject of further investigation by the same Department following a recommendation that a security clearance be granted. This approach could well amount to harassment and discourage military personnel in future from asserting rights that Parliament intended them to have.

Role of Counsel. Of the 21 complainants who appeared before us at hearings on security clearances, only four were assisted by counsel of their own. The rest were generally young people without the means to retain counsel.

We are concerned about a perceived or real lack of fairness when a department or agency of government, represented by counsel, faces a complainant who is alone, often nervous, seldom able to cross-examine effectively and, commonly, has little ability to make a cogent statement in his or her own defence. A low-ranking employee can be forgiven for feeling that he or she is not in a fair fight -- outnumbered, outranked and perhaps intimidated.

We believe that departments should ensure that their employees are represented by counsel, or at least an assisting official, at Committee hearings.

In the meantime, we have made it a practice to direct our own counsel -- whose first responsibility is to help us by interpreting procedural rules and the *Act* -- to give complainants what help they can, particularly by ensuring that all relevant evidence is brought forward and that appropriate questions are posed in direct and cross--examination.

Guidance to Security Officials. The Solicitor General has suggested that we make our decisions and the reasons for them more widely known within government. The more that security officials and senior managers understand the Committee's approach, the more likely they are to avoid pitfalls that lead to complaints.

At present, under the *Act*, our findings and recommendations in each case are communicated only to the complainant, the Solicitor General, the deputy head concerned and the Director of CSIS. Both privacy and security considerations are involved, since we ordinarily allude in our reports to personal information and often to classified official information.

However, we see great value in making our reasoning in decisions better known, and we are considering whether it may be possible to provide fairly detailed summaries, without names or sensitive information, to the security community, deputy heads and, perhaps, a wider public, including Parliament. Appendix C is a first step in this direction.

Complaints against CSIS

Mandate. The *Act* directs us to conduct investigations of complaints made about "any act or thing done by the Service". There are two principal limitations on the right to complain. A complaint must first be made to the Director of the Service. We can then accept the complaint if the Director has not responded within a period that we consider reasonable or if the complainant is not satisfied with the Director's response. Second, we may not investigate a complaint that can be channeled through another grievance procedure under the *Act* or the *Public Service Staff Relations Act*.

Official Languages. Almost all complaints made against the Service came from its own employees and focused on just two issues. The first was language policy. There were 480 complaints, filed by 21 persons, that internal documents were provided in English only, contrary to official languages policy requirements that these be made available simultaneously in English and French. These complaints were also filed with the Commissioner of Official Languages, D'Iberville Fortier. We are holding these complaints in abeyance while the Commissioner conducts an audit of the Service's official languages practices. We are co-operating with the Commissioner. Another nine complaints centred on linguistic issues.

Other Internal Issues. Of the remaining 49 complaints by Service employees, 45 came from a group of people who said through their counsel that their chances of promotion are unnecessarily limited. The reason alleged is that surveillance officers cannot transfer into investigation jobs. These complaints and the linguistic issue complaints are currently being considered by us as part of the special study requested by the Solicitor General on March 19, 1986, on the extent to which problems of bilingualism and personnel management are prevalent in CSIS.

Complaints from the Public. There were only four complaints against CSIS from non-employees. Three were beyond our jurisdiction and one is still under discussion with CSIS.

Immigration and Citizenship

Mandate. Under the *Citizenship Act*, the Secretary of State may make a report to the Committee when citizenship is denied because there are reasonable grounds to believe that the applicant is either a threat to the security of Canada or is involved in organized crime. Similarly, under the *Immigration Act, 1976*, a report may be made to the Committee when the Minister and the Solicitor General believe that an applicant for admission to Canada will engage in activities inimical to Canada's interests in various specific ways. In both cases, the individual about whom a report is made must be notified. We investigate as we would in the case of an individual complaint and make recommendations to the Governor in Council.

Referrals. One immigration case and 13 citizenship cases were referred to us. All were still under investigation at year-end, having only been received toward the end of the year.

Human Rights Cases

Mandate. When a minister advises the Canadian Human Rights Commission that the practice to which a complaint of discrimination relates is based on security considerations, the Commission can either dismiss the complaint or refer it to us. The complainant must be notified. When we receive such a referral, we consider whether the security concern is justified. After investigation, we report our findings within 45 days both to the Commission and to the minister concerned.

Referral. In 1985-86, one such case was referred by the Canadian Human Rights Commission, and a report was made within the statutory 45 days, advising the Commission that in our view the security considerations raised by the minister were justified.

Issues Arising out of Complaints

Notification. We became aware of a gap in the *Act* when a public servant was routinely investigated before renewal of his security clearance. Because of new information uncovered in the investigation, the security clearance was withdrawn. However, the department concerned also decided that a security clearance was not needed for the position in question.

Thus there was no immediate effect on the public servant's employment, and the department concluded that there was no need for notification. Indeed, the *Act* does not provide that public servants must be notified when a security clearance is denied -- only when a decision is made for security reasons to deny employment or to dismiss, demote or transfer or to deny a promotion or transfer.

However, this public servant's future promotions were jeopardized by withdrawal of the clearance, and he came to us when he inadvertently discovered what had happened. In the spirit of the *Act*, we persuaded the deputy minister concerned to issue official notification of a security clearance denial, thus clearing the way for a formal appeal. The appeal was, in fact, made and dismissed.

Exempt Staff. As written, the *Act* makes it difficult in some cases for us to investigate complaints from "exempt staff" -- that is, persons who work in ministers' offices. The *Act* provides for notice when an employment-related decision is made by a deputy head, but exempt staff is not generally under the authority of deputy heads. We do not believe that Parliament intended to deprive exempt staff of the right to appeal the denial of security clearances.

Conclusion

We, CSIS and many departments and agencies went through an intensive learning experience as complaints were investigated. We have no hesitation about committing all available resources to deal with cases quickly. National security considerations are of the highest concern, and so is the damage that problems with security clearances can do to individual lives.

However, we hope that a growing recognition in departments and agencies of the difference between security concerns and other personnel problems will soon bring about a reduction in the number of complaints. (It is not the fault of CSIS if this confusion created problems, as CSIS plays a "servicing" role; CSIS gets involved only at the request of a department, not on its own initiative.) We do not believe that Parliament intended the review process to be clogged with complaints founded on lifestyle problems like the abuse of alcohol and occasional soft drug use. These are matters of concern to employers, no doubt, but they seldom represent real threats to the security of Canada.

IV. Reaching Out and Settling In

While oversight and the investigation of complaints are the two main statutory duties we have, they do not, of course, stand alone. Obviously, we must be concerned with our own administration. And we must interact with others, inside and outside the intelligence community, in a number of ways.

Two closely related themes are communications and liaison. As described in detail below, we met with academic and other specialists, union officials, lawyers who may act as Committee counsel, government officials and knowledgeable Members of Parliament, and with our counterparts in the United States and the United Kingdom.

At some of these meetings, we were reaching out. That is, our principal goal was to let people know that we are available to investigate complaints in security matters.

Other meetings were arranged primarily as part of the process of settling in. Formal security intelligence oversight is new to Canada, and 1985-86 was our first full year of operation. Thus, a major preoccupation was to establish contacts and to build the perspectives and the fund of knowledge that will guide security intelligence oversight for years to come.

Communications is a two-way street; we learned from those we sought to inform, and we took pains to explain our work to those from whom we sought information.

Parliamentary Liaison

We kept lines to Parliament open. In addition to ongoing consultations with the Solicitor General, we met with Robert Kaplan, a former solicitor general and justice critic of the Liberal Party, Svend Robinson, justice critic of the New Democratic Party, and with two former solicitors general who still sit in the House of Commons, Warren Allmand, a Liberal, and Allan Lawrence, a Progressive Conservative.

At the time of writing, the Chairman was scheduled to appear before the House of Commons Standing Committee on Justice and Solicitor General on June 3, 1986, to discuss last year's annual report.

Reaching out to Public Servants

Because of stringent security requirements for many positions in the Public Service of Canada, public servants are likely to account for the bulk of complaints about denial of security clearances. So we made special efforts to ensure that public servants know of the review procedure.

Meetings with Union Officials. In August and September, we staged a series of meetings with representatives of unions that bargain for public servants and with the Public Service Commission of Canada. A list of participants can be found in Appendix D.

While the primary intention was to ensure that union officials know of the complaints procedure available to their members, we also invited them to keep us informed of security issues they encounter in their work.

Pay Envelope "Stuffer". Then we arranged through Treasury Board to have a brief introduction to our procedures distributed with paycheques on November 15 and November 22, 1985, to public servants nationwide. More than 350,000 copies were distributed in this way. The text can be found in Appendix E.

This notice is known to have brought 120 inquiries. The vast majority, 105, were satisfied with general information. But 15 people sought detailed information and two brought formal complaints to us.

A similar notice was printed in Canada Post's employee newsletter, and it brought a number of general inquiries.

Briefings and Consultations

We met with the Solicitor General, who has also been in touch with the Chairman on a number of specific issues.

Close relationships have also been maintained with the Director of the Canadian Security Intelligence Service, Ted Finn, and with the Inspector General, Dr. Richard Gosse. And we have been briefed by the Intelligence and Security Co-ordinator of the Privy Council Office, Blair Seaborn.

In addition, a number of people shared their special knowledge with us -- Mr. Justice David McDonald of the Supreme Court of Alberta, who was chairman of the Royal Commission concerning Certain Activities of the RCMP; Professor Peter Russell of the University of Toronto, who was research director of the same Royal Commission; and Jean Keable, who was chairman of Quebec's Commission d'enquête sur des opérations policières en territoire québécois.

Meetings with CSIS Staff. We toured the Service's offices in Toronto, Montreal, Vancouver, Quebec City and Ottawa, meeting with staff in those locations and being briefed on regional operational activities.

At each stop, the Chairman made a presentation to CSIS personnel on our mandate and philosophy and we entered into discussion with them.

In Toronto we examined the region's new, modern accommodations and were briefed on current operations and the allocation of the region's personnel resources to various responsibilities.

A full briefing from senior management in Montreal led us to believe that the workload in the area had increased considerably faster than the resources available. We also recognized that there were tensions regarding language use and personnel matters which probably exacerbated the imbalance between responsibilities and resources, and we decided at the end of the day to re-visit Montreal as soon as possible for a more detailed review of the situation there.

In British Columbia, we toured the Expo 86 site in December, 1985, with the Fair's Chief of Security. Following this examination of potential security problems and the precautions being put in place, we asked CSIS senior staff questions related to the Service's role in helping prevent terrorist or other incidents at Expo. We were particularly pleased to see the close co-ordination taking place between the various police forces involved and CSIS in the British Columbia region.

We were also given a full briefing on the British Columbia region's responsibilities, current operations, and resource concerns.

In Quebec City, we found that many investigators were concerned about the lack of written arrangements between the Service and other government departments and police forces. The contention was that basic factual information could not be easily obtained.

At the Ottawa regional office, we were advised of the heavy workload because of the large number of security clearance investigations being handled. We were also briefed on tradecraft matters and had an opportunity to view an ongoing operational activity and visit an operational location.

In addition, individual members of the Committee reviewed files in the CSIS offices in Ottawa, Quebec City, Toronto and Winnipeg.

Inspection of Training Facilities. In early March, we inspected the Sir William Stephenson Academy at Camp Borden, the Service's new training facility for intelligence officers. We were briefed on the curriculum and program by the Academy's Director General and senior instructors, and we met with students.

Foreign Experience

As the security intelligence oversight process takes shape in Canada, we are anxious to benefit from the experience of other countries and to establish personal links that will remain valuable for many years. With this in view, we made a two-day visit to Washington in October, 1985, and the Chairman and the Executive Secretary went to London in September, 1985, for briefings.

United States. In the United States, legislators have not delegated oversight to an independent body like Canada's Security Intelligence Review Committee but have kept it in their own sphere. Each house of Congress has an oversight committee composed of its own members -- the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

It was evident from discussions with members of both these bodies that their mandates differ significantly from ours. For example, the U.S. committees approve the budgets of their intelligence agencies. We do not perform this task with respect to CSIS. On the other hand, the United States has no counterpart to our mandate to hear complaints from public servants who are adversely affected in their employment as a result of denial of a security clearance.

It was also noteworthy that in the United States, a very large number of people are privy to very sensitive documents, whereas the numbers in Canada remain relatively small. It is obvious that the interplay between the intelligence community and the oversight bodies in the United States is highly complex and delicate, as the Yurchenko case demonstrated by provoking heated public debate late in 1985 between the chairman of the Senate committee and the director of the CIA.

During this visit, we also met officials of the Federal Bureau of Investigation. We intend to continue our liaison with the U.S. oversight committees and hope to meet too with officials of the Central Intelligence Agency, the Intelligence Oversight Board, and the President's Foreign Intelligence Advisory Committee in 1986-87.

We took advantage of our presence in Washington to meet with the Canadian Security Intelligence Service's liaison officer there and were briefed on his duties.

United Kingdom. No single legislative act governs the oversight function in the United Kingdom. But there are, nonetheless, a series of established and informal review mechanisms within the British intelligence community, and, taken together, they provide a function similar to that in Canada.

The Chairman and Executive Secretary were given access to key decision makers in the process and were able to share aspects of the Canadian oversight experience, which was of interest to U.K. officials from a parliamentary perspective.

Briefings were received from the CSIS liaison officers in London about their duties in the United Kingdom.

Academic Seminar

In October, 1985, we invited about two dozen Canadian professors in relevant disciplines and other experts to a seminar where we could draw on their knowledge and perspectives. This seminar was also attended by a representative of the U.S. Attorney General's Office of Intelligence Policy and Review, the Inspector General and a representative of the Privy Council Office. A list of guests can be found in Appendix F.

Consultations took place in the context of discussion of five specific papers centred on the theme of security intelligence in Canada in the 1980s. These papers are available from the Committee on request.

There was consensus that the Service should be concerned with full respect for democratic rights as well as effective security intelligence gathering. Indeed, there was broad agreement on many things -- that the Committee use its influence to raise the quality of analysis in CSIS' operations, for example, and that the Committee maintain a close relationship with Parliament.

We were interested to find that we were not alone in sensing a danger that the oversight function could be unintentionally neglected if we face a heavy load of complaints. This concern was also raised at the seminar. We are alive to the need to give due attention to both aspects of our mandate.

There were specific suggestions that we examine the Service's financial needs, doing a cost-benefit analysis of activities from time to time, and recruitment and training programs. Both these issues are addressed in Chapter II.

Counsel Seminar

In early March, 1986, a one-day seminar was held with 27 lawyers from across the country who are on call to act for us in complaints matters (and so all have Top Security clearances). Senior officials from the Department of National Defence and CSIS also attended. Participants are listed in Appendix G.

Presentations and discussion centred on the complaints process and the unique role that Committee counsel plays at hearings. Since complainants frequently appear without legal representation of their own and are generally unaware of the review procedures, Committee counsel must often assist the complainant as well as assisting us. Counsel also carry a heavy responsibility in helping determine what evidence or information can be divulged to a complainant to ensure procedural fairness without risking Canada's national security -- a process often requiring extensive negotiations among counsel participating in a case.

Participation in Conferences

In April, 1985, the Chairman, the Honourable Ronald G. Atkey, P.C., Q.C., together with the Executive Secretary and the Co-ordinator of Communications, attended a conference on "Freedom of Expression" held at the University of Western Ontario.

The Honourable Frank McGee, P.C., the Executive Secretary and the Coordinator of Communications participated in a conference organized by the Canadian Association for Security and Intelligence Studies at McGill University in May, 1985.

In March, 1986, the Honourable Jean Jacques Blais, P.C., Q.C., presented a paper entitled "Response to Terrorism in a Democratic Society" at a University of Ottawa conference on "International Terrorism".

Committee Personnel

Staff rose to its full complement of 13 by the time the fiscal year ended on March 31, 1986, up from three at the beginning of the year, on April 1, 1985. Staff members are listed by name and position in Appendix H. Every effort will be made to keep the number of employees at the present level.

Because few employees worked the full year, the number of person years used in 1985-86 was only eight.

Since much of the information that crosses the desks of staff is highly sensitive, we have asked CSIS itself to clear all of them to the Top Secret level.

Financial Report

Spending in 1985-86 was as follows:

Personnel	\$339,000
Salaries and wages	\$293,000
Contributions to employee benefit plans	\$46,000
Operating Expenses	<u>\$537,000</u>
TOTAL	\$876,000

V. Major Policy Issues

In our deliberations during the past year, we have identified and considered a number of key policy issues for decision by the Government or Parliament.

Foreign Operations

Section 16 of the *Act* provides for collection of information concerning foreign states and persons through operations within Canada. These duties and functions, before being performed, must be personally requested by either the Minister of National Defence or the Secretary of State for External Affairs with the consent of the Solicitor General. No such collection of information by CSIS has taken place as yet, but the Government is currently considering how and when it might use the powers granted by section 16.

This raises the broader policy issue of whether CSIS should be allowed to conduct information-gathering operations abroad. This might require an amendment to the *Act* by Parliament. We are mindful of the reluctance of Parliament and many Canadians to allow CSIS to take on the sort of covert functions performed around the world by the Central Intelligence Agency (CIA) on behalf of the U.S. government. On the other hand, some Canadians have asked why this nation continues to deny itself the benefits of an intelligence capability abroad when so many foreign intelligence agencies are operating offensively within Canada.

This is obviously a subject that Parliament might debate when it reviews the *Act* in about three years' time. At this point, we do not have a fixed position on this issue and simply want to signal it as a subject of future debate.

Government Employees, University Campuses

Other major policy issues currently under consideration by CSIS are the use of government employees as sources of information and investigations by CSIS on university campuses in Canada; CSIS discussion papers on these issues are currently before the Government. We will watch closely the evolution of the Service's position and may make them the subjects of future reports. Our guiding principle, as always, will be to seek to maintain the delicate balance in our democratic society between the intrusive powers of CSIS and the rights and freedoms of Canadians. CSIS has a genuine concern that its ability to operate in areas of Canadian society where hostile intelligence officers or their agents, terrorists or subversives are active not be limited.

Emergency Warrants

The *Act* specifies the procedures by which CSIS obtains approval for warrants from a judge of the Federal Court. No provision is made for a special, more limited procedure in emergency situations, because it was expected that by accelerating the standard procedure, warrants could be obtained quickly enough to satisfy all contingencies.

Under the *Official Secrets Act* warrants could be obtained in about three hours. We understand that the *Canadian Security Intelligence Service Act* procedures make such speedy approval virtually impossible now. Though no specific instances of operational problems caused by delays in obtaining warrants have been cited to us, CSIS management's judgment is that an emergency warrant approval process is necessary.

For example, such a process might be used where CSIS obtained information at the last minute about the stop-over between flights of a suspected terrorist at a Canadian location. An emergency warrant would allow a meeting to be monitored, whereas the present process would so delay the approval of a warrant that the meeting could not be monitored. In counter-terrorist activity especially, the reaction speed of the government must match the volatile activity and carefully contrived precautions of the terrorists.

We believe that exceptional situations or threats may require exceptional measures. Parliament may wish to consider, therefore, an amendment to the *Act* which would provide for short-term emergency warrants to be authorized in exceptional circumstances by the Director. Such warrants would, of course, be reviewed and confirmed or cancelled by a Federal Court judge within, say, 48 hours. As a further safeguard, any use of these emergency powers by the Director could be required to be reported to the Solicitor General and to the Review Committee within a specified time.

Other Issues

Some further policy issues that might be considered by Parliament in future through legislative amendment are listed below.

- Is the definition of "threats to the security of Canada" in section 2 of the *Act* too broad, particularly insofar as it sustains the somewhat controversial counter-subversion program of CSIS? We will be addressing this policy issue in the coming year.

- Should the Canadian Armed Forces be exempt from Part III of the *Act* on the basis that the adjudicative procedures provided there are inappropriate for complaints from military personnel about the denial of security clearances? This position is being advocated within the Department of National Defence, but we do not support it.
- Is there some way that CSIS can warn voluntary organizations when they are being infiltrated by persons who may subvert them for purposes that could represent a threat to the security of Canada? To avoid needlessly tarnishing the reputations of persons who have as yet committed no crime, CSIS is limited in what it can say. But loyal Canadians who belong to groups threatened with subversion deserve to be alerted if some means can be found of communicating appropriate information. Also, is there some way in which individuals who join a "front organization"* because they support its overt aims, can be warned of the organization's covert objectives?

* One definition is: "an outwardly independent organization whose promotion of idealistic, humanitarian and non-partisan political issues serves to obscure its covert objective of promoting public support for policies and initiatives of the organization or foreign power by which it is controlled. Membership in a front organization should not be construed as knowledge of, agreement with, support of or adherence to, the organization's covert objectives."

Appendix A

Research Study on Canadian Security Intelligence Service Recruitment, Training and Development Programs -- Executive Summary

In last year's annual report, we indicated that the examination of CSIS' training and development activities would be a priority. After a briefing from CSIS on this matter, we decided to undertake a full research study, which was completed in March, 1986, and forwarded to the Solicitor General, the Director of CSIS and the Inspector General.

The study compares recruitment, training, and related matters in CSIS and the RCMP Security Service, making extensive reference to findings in Chapters I and 2 of Volume II of the McDonald Commission report, "Freedom and Security under the Law". We interviewed 165 CSIS employees chosen at random, met with inductees into the CSIS intelligence officer training program, and were briefed by CSIS staff and senior management and by other government and non-government experts.

Findings and Recommendations

In the RCMP Security Service, training and recruitment followed a career service model and a generalist orientation. In operations -- that is, everything other than administration or support -- almost all promotion to middle and senior management was through the ranks. An officer usually stayed at a position for only two or three years and was transferred regularly to new posts requiring new knowledge and skills.

CSIS continues to maintain a career model, encouraging entry at the bottom and promotion through the ranks in the operational areas. We recommended entry by a limited number of qualified individuals from outside the Service into middle and senior operational positions.

CSIS has taken a number of measures to encourage specialization, including specialist pay supplements and a job classification system that permits promotion without transfer. We were supportive of these measures, but noted that the new competition system, by encouraging job transfer, might work against specialization. We recommended that CSIS monitor the effects of the competition system on specialization and job continuity.

Prior to transition, the Security Service recruited among serving RCMP officers. CSIS is now recruiting for operational positions outside of the RCMP. In selecting its first batches of recruits, CSIS did not advertise but relied upon employment applications, the majority of which had been received by the RCMP prior to transition. We recommended that CSIS advertise widely for recruits so that the Service could develop broadly based recruitment sources.

The Security Service, by recruiting in the main from the RCMP, tended not to hire university graduates or individuals from minority backgrounds. We examined the composition of the first CSIS intelligence officer class and found that all recruits were university educated. But the class did not include enough Francophones or women. Many had only limited French language capabilities and few knew any foreign language. We recommended that greater efforts be made to recruit Francophones and that the Service also examine the adequacy of its current recruitment program with respect to women. We suggested more recruitment of individuals with foreign language skills.

A caste-like division was maintained in the Security Service between "regular members" (RCMP officers) and civilians on its staff. "Members" in operational areas were promoted internally and entry into operational areas for civilians was limited. In CSIS, all positions are now subject to the same open competition, like all other public service positions. Employees in non-operational areas have been encouraged to become intelligence officers through a number of special conversion competitions. We found, though, that many employees in the operational areas were critical of the fairness of the competition process. We thus recommended that competition posters clearly indicate final selection criteria, that CSIS consider the use of "outsiders" such as Public Service Commission employees on competition boards, that CSIS introduce a career counselling service staffed by professionals, and that generally CSIS examine means of improving the competition process.

Some public servants in CSIS were concerned that CSIS' designation as a separate employer would end their current right to enter other public service competitions. We noted that CSIS is seeking, with the Public Service Commission, to rectify this situation, and recommended additional efforts in this area.

In the Security Service, all intelligence officers were subject to the para-military training and "parade square" discipline of the RCMP, with an emphasis on police investigation. CSIS has developed a new training program for recruits to the intelligence officer stream that dispenses with such discipline and emphasizes security work. The program received a very high rating by the first class of recruits. While we were unable to fully examine the content of courses, and so had few suggestions for improvement, we recommended that additional time be spent on federal statutes, including the *Criminal Code*, and the *Act*. We also recommended that training courses be made available in French without delay.

Regarding in-house courses, CSIS, like the RCMP Security Service, has a very limited number and variety. Intelligence officers criticized the lack of tradecraft courses, and hoped that more such courses would be made available. Outside the intelligence officer stream, other groups equally criticized the adequacy and number of available courses. However, we did hear favourable remarks about a new inductee training program designed to make non-operational employees feel like "part of the Service". In our report, we recognized that, initially, resources have been aimed at training new intelligence officers, and suggested that extra effort now be put on developing in-house training programs.

CSIS, like the RCMP Security Service, offers few secondments and other developmental opportunities, and consideration of such opportunities is not an integral part of the employees' annual review process. Most individuals interviewed had had no such opportunities, but those who had were quite satisfied with them. We recommended that training and developmental needs be identified on an annual basis, that these needs receive more emphasis in the employee annual review process, and that plans made in response to them be reviewed on a regular basis to ensure implementation.

Before transition, the facilities available to employees with emotional problems were characterized as "primitive" and "unavailable", and the McDonald Commission recommended an employee counselling program based on the principles of voluntary use and confidentiality. Little has changed in CSIS, and we, therefore, recommended that an employee assistance program be instituted, that the program be staffed by professionals with adequate rank to deal with all levels of employee, and that the availability of this program be communicated to all employees.

In examining the composition of the old Security Service, the McDonald Commission indicated that it had only three officers above the rank of inspector whose first language was French. Francophones continue to be under-represented among CSIS' recruits and in senior positions. We found instances of alienation and discontent among Francophone intelligence officers. We also noted a general lack of urgency within CSIS in making available services and documents in French. We recommended that more Francophones be hired at senior levels and that all communication with Québec and all documentation for national use be available in French. We further recommended that emphasis be placed on bilingualism as a recruitment criterion and that senior management recognize -- and commit itself to -- implementing the Government's bilingualism policy.

The report concludes with an examination of morale among CSIS employees. We found problems in a number of areas, some of them due to transition difficulties. We suggested that better communication between senior management and employees might alleviate some of these problems, and recommended that senior management build an organizational culture that stresses people as its most important resource.

CSIS management has displayed a great deal of effort in the transition process, with good results in a number of areas. We were particularly impressed with the involvement of senior managers in detailed training, personnel and development planning, and in the speed and efficacy with which the new intelligence officer training program was implemented. We believe, nonetheless, that a number of areas urgently require attention, and highlighted these areas in our recommendations.

Appendix B

Ministerial Directives since July 16, 1984

July 16, 1984	Foreign Operations -- Request for the Completion of a Draft Policy from CSIS
July 18, 1984	Delegation of Financial Authority to CSIS
July 20, 1984	(Secret)
July 29, 1984	Guideline of the Principles on which the Security Responsibilities of the RCMP and the CSIS Should be Based
Aug. 24, 1984	Delegation of Authority to Designated CSIS Officials for the <i>Access to Information and Privacy Acts</i>
Aug. 28, 1984	Continuity of Ministerial Policy Direction Applicable to the RCMP Security Service, for CSIS (not inconsistent with <i>CSIS Act</i>)
Sept. 10, 1984	(Top Secret)
Nov. 16, 1984	CSIS to Consult with the Solicitor General Prior to Advocating a Policy which Directly Relates to the Position of the Government
Dec. 4, 1984	(Top Secret)
Dec. 5, 1984	Delegation of Authority under s. 178.18(2)(d) of the <i>Criminal Code of Canada</i> . (Solicitor General to authorize designated CSIS officials to sign licences for persons to possess, sell, purchase electronic devices for surreptitious interception of private communications)
Feb. 5, 1985	(Secret)
Feb. 15, 1985	Revised Delegation Orders -- <i>Access to Information and Privacy Acts</i>
Feb. 15, 1985	Agreements (Memorandums of Understanding) with the RCMP in Operational Areas
March 5, 1985	Changes to CSIS Collection, Retention and Destruction Procedures for Files in the CSIS Exempt Bank

Appendix C

Summaries of Security Clearance Complaints on which the Committee has Reached Decisions

Public Service

1. An individual filed complaints against the RCMP and CSIS alleging discrimination in the provision of services on the grounds of ethnic origin.

The Solicitor General forwarded to the Canadian Human Rights Commission a written notice which indicated that the facts in both complaints involved matters relating to the security of Canada. The Commission then referred the complaints to the Committee.

The Committee found that the written notice provided by the Solicitor General was substantiated by the facts of the case, and that there were no grounds to justify the allegations of discrimination by the complainant.

2. An individual complained that a security clearance had been withdrawn and that, as a consequence, the individual had been suspended indefinitely without pay.

The Committee found that the Department should have treated the case as a strictly personnel management matter, not as a national security issue, and recommended that the deputy head take all necessary action to permit the complainant to present a grievance before the Public Service Staff Relations Board.

3. An individual complained that a security clearance had been denied on the basis of lifestyle considerations which were no longer relevant.

The case focussed on the individual's use of drugs, association with drug users, and association with known criminals.

The Committee found that the facts of the case supported CSIS' allegations about the previous lifestyle of the complainant, but considered that the individual's way of life had recently taken a dramatic turn for the better.

The Committee recommended that the CSIS recommendation be sustained but the complainant be reconsidered for a Top Secret clearance in two years.

4. An individual complained that a job offer had been withdrawn because the deputy head had accepted a CSIS recommendation that a Secret clearance be refused.

The case centered on the individual's associations with persons suspected of being agents of other countries, and the CSIS assessment that classified information might be given to unauthorized persons if a security clearance were granted.

The Committee examined seven specific allegations. It concluded that one allegation concerning events of over 10 years ago was substantiated, and that the remainder were without foundation. It recommended that the deputy head grant a Secret clearance and offer employment in the previously agreed position to the complainant.

5. An individual complained that a security clearance had been denied and that, as a consequence, promotion in the Public Service would be much less likely.

The Committee assumed jurisdiction after hearing arguments. Though there were no immediate employment implications, the Committee and the parties concerned recognized that there would be a severe effect on the complainant's career potential.

The case centered exclusively on the complainant's association with a Marxist-Leninist group.

The Committee discovered that the platform of the Marxist-Leninist group, with which the individual was associated, included the use of violence to assist in the overthrow of Canada's present system of government. It found that association with a group espousing the use of violence against our system of government cast doubt on the individual's loyalty to Canada. The Committee recommended that the denial of a security clearance be undisturbed.

Department of National Defence

6. A member of the Forces complained that a security clearance was denied on the basis of behaviour during adolescence which was no longer relevant to the granting of a security clearance.

The Department of National Defence cited behaviour ranging from delinquency at age 12 through episodes of criminal behaviour to a conviction resulting in a compulsory stay of 28 days in a detoxification centre at age 18.

Testimony showed that after this latter episode, the complainant became a drug counsellor, resumed a high school education program, and then joined the Canadian Forces where superior performance evaluations were awarded by commanding officers. The complainant's use of alcohol did not cease during this period, but alcohol consumption was reduced to a level equal to or below that of the complainant's peers.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee recommended that a Secret clearance be awarded and that the complainant's reliability be monitored to ensure that alcohol abuse did not again become a problem.

7. A civilian employee complained that a Secret security clearance had been withdrawn.

The Department of National Defence testified that the complainant worked as a prostitute and was highly susceptible to coercion by another individual. It was not the prostitution itself but the vulnerability to manipulation by another person that persuaded the Department to remove the Secret security clearance.

The complainant testified that becoming a prostitute was the result of extreme financial pressure, but that continuing to work as a prostitute was the result of the fear of physical beatings by another individual.

The Committee recommended that the complainant be offered a job in another area, well away from the influence of the individual who had inflicted the physical violence, and be reconsidered for a security clearance in two years.

8. A member of the Forces complained that a Top Secret security clearance had been withdrawn, and no level of security clearance granted.

The Department testified that during a six-month period in 1984 the complainant was convicted of a number of offences under provincial legislation and the *Criminal Code*. These incidents together with an alleged breach of security under the influence of alcohol led the Department to deny any level of security clearance.

The Committee found that the Department's decision was substantiated by the evidence but, in view of a marked improvement in behaviour, recommended that a review of the complainant's security clearance status be conducted earlier than planned, and, in any event, no later than August, 1986.

9. A member of the Forces complained that a Cosmic Top Secret clearance had been withdrawn and a clearance no higher than Confidential awarded.

The Department asserted that financial and family circumstances, together with the undue influence of the complainant's spouse, created a situation where advances by agents could be successful. There was no suggestion that any such advances had been made.

Evidence adduced at the hearing showed that the complainant had been coping well with financial and family difficulties, which were not of the complainant's own making, for some time.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee also found that there was insufficient reliable and current information before the Department's Security Clearance Junior Review Board (SCJRB) to justify the conclusion to which it came. The Committee recommended that a new field investigation be carried out immediately and that the complainant's Top Secret security clearance be reconsidered by the SCJRB as soon as that investigation was completed.

10. A member of the Forces complained that a Top Secret security clearance was withdrawn and a clearance no higher than Confidential was awarded in its place. This action required the member to change his employment from one trade to another and, as a consequence, to be demoted to a lower rank.

The Department asserted that behaviour overseas led to the conclusion that the complainant may have been approached or subverted by a hostile intelligence service. This departmental view was alleged to have been supported by the results of polygraph examinations which the complainant volunteered to undergo.

Evidence before the Committee showed that, after conducting an investigation, the Security Service of the RCMP did not believe that the complainant had co-operated with a hostile intelligence service nor did it have reason to believe that this might happen in the future. Despite this conclusion by experts in the field, the Department denied the complainant a Top Secret security clearance on two separate occasions.

The Committee concluded that though the complainant had used alcohol excessively for some years, there was no evidence to support the allegation of co-operation with a hostile intelligence service. It recommended that the complainant be granted a Top Secret security clearance and be restored to the higher rank previously held.

11. A member of the Forces complained that a Secret security clearance had been withdrawn and a clearance at any level had been denied.

The Department asserted that in December, 1984, the member had admitted to using hashish on six or seven occasions since enrolment in the Canadian Forces in May, 1983. Because this use of hashish was a breach of the Armed Forces drug policy, the Department concluded that the member would not be reliable in other circumstances and should not be given any level of security clearance. The Department admitted that there was no adverse information before the Security Clearance Junior Review Board other than the breach of the drug policy.

The evidence showed that the member had not used drugs since early 1985, and had used soft drugs on a very occasional basis in previous years.

The Committee concluded generally that though even minor use of drugs was a breach of the drug policy and was a serious matter which could be taken into account by the Canadian Forces in its role as an employer, it did not, in and of itself, signify a defect of character such as would so seriously affect the member's reliability as to render the member unqualified to hold a security clearance.

The Committee found, therefore, that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee recommended that the complainant's Secret security clearance be restored.

12. A member of the Forces complained that a security clearance of Top Secret was denied and a Secret clearance awarded in its place. This action made it almost impossible to progress in the member's military trade.

The Department asserted that the member's use of marijuana on three occasions in 1983 warranted the denial of a Top Secret security clearance. Once again (as in # 11 above), the Department essentially based its case on the fact that the member had breached the Armed Forces' drug policy and had, therefore, shown a lack of reliability sufficient to warrant the withdrawal of a Top Secret security clearance.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee explained its general position as follows:

Therefore, though I find it plausible that the Canadian Forces would have stringent rules and severe sanctions regarding the use of drugs by military personnel, I do not believe that this general policy can be extended to assert that military personnel are more likely to reveal secret information than are civilians who consume equal (limited) amounts of soft drugs. The quantity of drugs consumed by [member] would not have led to a civilian being denied a Top Secret security clearance. I find, therefore, that this limited use of drugs does not, of itself, provide a sufficient basis for the decision to deny [member] a Top Secret clearance. Nor, having regard to all the evidence can I conclude that [member] otherwise has a defect of character that would justify concerns about [member's] reliability from the perspective of national security.

The Committee recommended that the complainant be granted a Top Secret security clearance.

13. A member of the Forces complained that a security clearance had been denied, based on alleged possession and trafficking in drugs prior to enlistment, and unreliability. The complainant denied having concealed prior convictions, denied using drugs in recent years, and complained that no opportunity had ever been provided to explain or refute the Department's allegations.

The Committee noted that the drug trafficking allegations were built on unwarranted suppositions, and that drug use had occurred in youth, during a difficult period. Also, the Committee found that the complainant had in recent years received positive performance reviews, and had a pattern of exemplary service and behaviour.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee recommended approval of the requested Confidential clearance.

14. A member of the Forces complained that a security clearance had been downgraded based on incidents of drug use, destruction of military property, attempted suicide, and alcohol abuse. The complainant argued that all the incidents in question were alcohol related, and that he had undergone a successful alcohol rehabilitation program.

The Committee found that all the incidents had occurred when the complainant was under the influence of alcohol, and that he had successfully taken steps to deal with an alcohol problem.

The Committee recommended, therefore, that the Complainant's clearance be reviewed at the conclusion of a two-year period dating from the initial downgrading of the clearance.

15. A member of the Forces complained that a security clearance had been denied based on admissions of past and current use of illicit drugs, susceptibility to peer pressure and excessive alcohol use. The complainant argued that some statements were made under duress, and that some statements had been misunderstood by the investigator.

The evidence showed that the Department had overstated its case, and that the complainant had ceased using drugs.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee recommended reversal of a decision to deny any clearance, and approval of the sought-after level unconditionally or subject to future review.

16. A member of the Forces complained about a downgrading to nil security clearance following an investigation for a higher level clearance. The downgrading was based on drug use, alcohol abuse, and indebtedness.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee also noted that the individual had shown a demonstrated behaviour pattern of reform and rehabilitation over the latest two-year period.

The Committee recommended that the security clearance be granted.

17. A member of the Forces complained that a security clearance had been denied on the grounds of an alleged suicide attempt, adverse psychiatric evaluations, and a negative service record.

The Committee found that the alleged suicide attempt, which had triggered the investigation in the first place, was, in fact, unsupported by any evidence, and was denied by the complainant.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee also noted a significant improvement in the complainant's behaviour during the last two years.

The Committee recommended approval of the sought-after clearance, and further recommended that any member of the Forces downgraded or denied a clearance be told of the reason for that denial or downgrading within 30 days.

18. A member of the Forces complained that a security clearance at any level was denied because of alleged prior associations with known criminals, irresponsible behaviour, and abuse of alcohol.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee also found that the individual, since the incidents in question, had had an exemplary service record and above average evaluations from superiors.

The Committee recommended that the complainant be granted the security clearance requested.

19. A member of the Forces complained that a clearance was denied because of alleged personal traits, loose morals, and peers' antagonism.

The complainant denied all the allegations.

The Committee noted the lack of any opportunity given to the complainant to respond to the allegations, and the biases evident in the file record of the investigation.

The Committee found that there was no evidence to suggest that the complainant's loyalty to Canada, or reliability as it relates to loyalty, were sufficiently doubtful to warrant the denial of a security clearance.

The Committee recommended that a security clearance be granted.

20. A member of the Forces complained that a security clearance had been denied on the basis of allegations concerning discretion and stability. The complainant argued that religious beliefs and anti-nuclear views were the cause of the security clearance denial, and complained that this was unjust.

The Committee noted the right of Canadians to hold the views espoused by the complainant, but concluded that the strength of those beliefs made the complainant vulnerable to groups or individuals who had aims inimical to Canada's national security. The Committee recommended that the complainant's security clearance be restricted to Confidential.

21. A member of the Forces complained that a security clearance had been denied because of allegations concerning character traits. The individual was said to have wrongly used donations of money for his own purposes, and to have made sexual advances in situations which could have led to the complainant becoming vulnerable to blackmail.

The Committee examined all the incidents in question, noting that many were unsubstantiated, or mere hearsay. However, there was also evidence that the individual had not been forthright with the Committee, and had expressed allegiance to countries other than Canada, thus raising questions as to both honesty and loyalty.

The Committee recommended that the denial of the complainant's security clearance be maintained.

Appendix D

Union Representatives at Meetings with the Committee, August and September, 1985

Public Service Alliance of Canada Susan Giampietri, Second Vice- President	Council Bob Paterson, President, Broadcast Council
Renaud Paquet, National President, Canada Employment and Immigration Union	Canadian Labour Congress Neville Hamilton, Administrative Assistant to the President
Mansel Legacy, National President, Customs and Excise Union	John Harker, Director of the Inter- national Affairs Department
Phil Vincent, Service Officer, Taxa- tion Component	Economists, Sociologists and Statisticians Association
Patricia Elliott, Service Officer, Union of Solicitor General Employees	Jack MacKinnon, President
David Green, Service Officer, Union of National Defence Employees	Marvin Gandall, Executive Secretary
Denis McCarthy, Service Officer, National Component	Professional Institute of the Public Service of Canada Edward Spencer, Policy and Planning
Steve Jelly, Executive Assistant to the Executive Management Committee	Claude Leclerc, Manager, Legal Members Services
Louise Czernenko, Assistant to the President	Canadian Federation of Labour
Yolande Viau, Research Officer	J. McCambly, President Tim Catherwood, Officer
Mariam Edelson, Equal Opportunity Co-ordinator	Public Service Commission of Canada Maureen Stewart, Staffing Program and Program Development Directorate.
Canadian Union of Public Employees	
Pascal Ingenito, National Director of Organizing and Servicing	
Gordon Johnson, Director, Broadcast	

Appendix E

Text of a Notice Distributed to Public Servants, November, 1985

If you have been denied a security clearance which is required by the Government of Canada, and are, as a result, denied employment, dismissed, demoted, transferred, or denied a promotion or a transfer, the Security Intelligence Review Committee may be able to help.

The Review Committee was appointed on November 30, 1984, under statutory authority as an independent body representative of the three parties in the House of Commons. It is mandated by Parliament to review the performance of the duties and functions of the newly created Canadian Security Intelligence Service (CSIS) as well as to hear complaints from federal public servants who are denied a security clearance by a federal department or agency.

Hon. Ronald G. Atkey, P.C., Q.C.,
Chairman

Mr. Maurice Archdeacon, Executive
Secretary

For further information, visit, write or
telephone:

Security Intelligence Review Com-
mittee
16th Floor
365 Laurier Avenue West
Ottawa, Ontario

Mailing Address:

P.O. Box 2430
Postal Station 'D'
Ottawa, Ontario
K1P 5W5

Telephone: (613) 990-8441

You may call collect between
7:30 a.m. - 5:30 p.m., Ottawa time.

Appendix F

Academic Seminar, October 10, 1985

Guests

Alan Borovoy, General Counsel,
Canadian Civil Liberties Association

Jean-Paul Brodeur, Université de
Montréal, Criminology Department,
Past Director of Research for the
Keable Commission (unable to
attend)

David Charters, Assistant Director,
Centre for Conflict Studies,
University of New Brunswick,
Executive Committee Member of the
Canadian Association for Security
and Intelligence Studies

David Cox, Queen's University,
Department of Political Studies,
Director of Research for Canadian
Institute for International Peace and
Security

Ronald Crelinsten, Department of
Criminology, University of Ottawa

André Donneur, Université de
Québec à Montréal, Department of
Political Science (unable to attend)

J.L.L.J. Edwards, University of
Toronto, Law School

Stuart Farson, Department of
Criminology, University of Toronto,
Executive Committee Member of
Canadian Association for Security
and Intelligence Studies

C.E.S. Franks, Queen's University,
Political Studies Department

Richard French, McGill University,
Faculty of Management (formally
PCO), Executive Committee Member
of Canadian Association for Security
and Intelligence Studies

Martin Friedland, Faculty of Law,
University of Toronto

Richard Gosse, Q.C., Inspector
General

J.E. Harlick, Intelligence and Security
Secretariat, Privy Council Office

Richard Henshel, University of
Western Ontario, Sociology
Department

Mary C. Lawton, Counsel, Office of
Intelligence Policy and Review, U.S.
Department of Justice

Murray Rankin, Faculty of Law,
University of Victoria, B.C.

R.H. Roy, University of Victoria, B.C.,
Department of History, Chairperson of
the Canadian Association for Security
and Intelligence Studies

Peter Russell, University of Toronto,
Past Director of Research for the
McDonald Commission, Executive
Committee Member of Canadian
Association for Security and Intelligence
Studies

David Stafford, University of Toronto,
History Department, Executive
Committee Member of Canadian
Association for Security and Intelligence
Studies

Peter St. John, University of Manitoba,
Lecturer on Terrorism and Intelligence

André Tremblay, Faculty of Law,
Université de Montréal

Geoffrey Weller, Lakehead University,
Political Science Department

Appendix G

Legal Counsel Seminar, March 8, 1986

Committee Counsel	Mary E. Saunders, Vancouver
Gina S. Brannan, Toronto (unable to attend)	Perry W. Schulman, Q.C., Winnipeg
George T.H. Cooper, Q.C., Halifax	Graham W.S. Scott, Q.C., Toronto
Graham Charles Eglinton, Ottawa	John M. Sibley, Toronto
Morris J. Fish, Q.C., Montreal	J. Peter Vice, Q.C., Ottawa
Mark P. Frawley, Toronto	Grant Kenneth Weaver, Vancouver
Pierre-C. Gagnon, Quebec City	Alan Whiteley, Toronto David L. Zifkin, Toronto
Edward L. Gladu, Q.C., Ottawa	Canadian Security Intelligence Service
Gordon Grey Hilliker, Vancouver	Ray Lees, Deputy Director -- Regional Operations and Liaison
William G. Horton, Toronto	Bob Duff, Director General -- Toronto Region
Robert E. Houston, Q.C., Ottawa	Barry Denofsky, Standing Requirements
John B. Laskin, Toronto	Cliff Percy, Chief -- Briefing Unit
Jack R. London, Q.C., Winnipeg	
Allan Lutfy, Q.C., Ottawa	CSIS Counsel
Robert W. MacQuarrie, Q.C., Ottawa	Douglas R. Wyatt
Eva Marszewski, Toronto	Department of National Defence
Edouard Martin, Québec (unable to attend)	Lt.-Col. Paul Corban
Mel Myers, Q.C., Winnipeg	Guest Participants
Simon Noël, Hull	Jan Dymond, Toronto
Christopher J. Roper, Toronto	Eleanore A. Cronk, Toronto

Appendix H

Security Intelligence Review Committee Staff

Maurice Archdeacon, Executive Secretary	990-6839
Yvette Collins, Senior Secretary	990-8442
Danielle Blache, Junior Secretary	991-9112
Shirley Heafey, Executive Assistant (Complaints)	993-4263
Jacques J.M. Shore, Director of Research	990-8051
Maurice M. Klein, Research Officer	990-8445
John M. Smith, Research Officer	991-9111
Joan Keane, Research Assistant	990-8443
Annie Demirjian, Co-ordinator of Communications	990-6319
Madeleine DeCarufel, Administration Officer and Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, File Clerk	990-6838
Diane Marion, Receptionist-Secretary	990-8441