SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1987-1988

Security Intelligence Review Committee
14th Floor
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
KIP 5W5

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

Minister of Supply and Services Canada 1988
Cat. No. JS 71-1/1988
ISBN 0-662-56247-X

September 30, 1988

The Honourable James F. Kelleher, P.C., M.P., Q.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
KIA OA6

Dear Mr. Kelleher:

Pursuant to section 53 of the *Canadian Security Intelligence Act*, we hereby transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1987-88, 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.

Turning the corner

Contents

1. A Second Wind

We hope our successors will be able to look back and say that 1987-88 was the year the Canadian Security Intelligence Service (CSIS) turned the corner.

It was a year in which CSIS faced perhaps its darkest moments, capped by the resignation of its first Director after the Atwal warrant affair (see page 11). With the requirement for secrecy that is central to its operations, CSIS cannot have been pleased about the number of "outsiders" who came through its doors. First there was the Independent Advisory Team, armed with the conclusions of our last Annual Report and our special report on official languages and staff relations, *Closing the Gaps,* together with a mandate for change.* Then came a new Director appointed from outside the Service. The counter-subversion branch was disbanded and its duties reassigned. Even though operational work was not significantly affected, no one could blame the men and women of CSIS if they were sometimes frustrated.

But there is an up side to all of this. The Independent Advisory Team developed a realistic reform package on the basis of our recommendations, and the Government started to implement it. Disbandment of the counter-subversion branch will stem overreaction to the rather modest threats Canada faces from home-grown radicals. Early indications are that the new Director is providing active leadership.

In short, we feel that this difficult year brought CSIS the chance it needs to get a second wind and complete its evolution into the kind of agency that Parliament intended when it adopted the *CSIS Act* in 1984--a civilian agency with contemporary priorities, its attention focused on gathering and analysing security intelligence as a basis for solid advice to the government of the day.

Good Calls and Bum Raps

Some of the barrage of criticism CSIS faced last year was justified. Haste does not excuse the carelessness that allowed unreliable information to be used in obtaining Federal Court authority for the Atwal wiretap.

But nemesis was at work, and the Atwal affair brought its own punishment. Because of the flawed warrant, proceedings had to be suspended against five men accused of conspiracy to murder a minister of the state government of the Punjab in India. CSIS also came under public fire for failing to inform police in advance of the conspiracy. Conversations recorded in the wiretap pointed clearly to a plan to assault the minister, but CSIS did not review the material until the attempt had already been made.

---

* The Independent Advisory Team was appointed by the Solicitor General on July 22, 1987, and handed in its report, *People and Process in Transition,* with 34 recommendations, on October 28, 1987. Headed by Gordon Osbaldeston, a former clerk of the Privy Council and now a senior fellow at the School of Business Administration, University of Western Ontario, it also included Roger Tassé, a former deputy solicitor general and deputy minister of justice who now practices law privately, and Gérard Duclos, Deputy Controller General, Management Review Branch, Treasury Board.

This episode also contributed to an atmosphere of suspicion--not to say derision--in which all sorts of allegations about bungling and wrongdoing were floated. Looking into media reports and following up our own leads, we found that much of what was being said was mistaken. We found that:

- CSIS did *not* slip up in the entry into Canada of Mahmoud Mohammad Issa Mohammad; someone did, but it was not CSIS.

- *Nor* did it compromise his attempt to leave the country.

- There is *no* evidence to date that CSIS had usable and reliable information that might have prevented the Air India tragedy of June 23, 1985, when a jumbo jet bound from Toronto and Montreal to Bombay went down off the coast of Ireland at a cost of 329 lives; to have said that trouble was likely on an aircraft of Air India was good common sense but hardly a "tipoff" to a specific event.

- *Nor* was there any basis to conclude that there was a loss when wiretap tapes were routinely erased after the relevant information they provided had been noted.

- CSIS does not target the labour movement.

- It did *not* try to get the *Sûreté du Québec* to give one of its informers a break in the investigation of bombing incidents.

- Complaints to the media as well as to us by a man that he was being harassed were *not* founded; after investigation, we concluded that CSIS made reasonable inquiries in a reasonable way.

CSIS had its successes too. Unfortunately they are measured on an invisible scale--by what does not happen rather than by what does. But fair is fair. It is only fair to remember that 1987-88 was a year of unusually heavy demand for security intelligence as Canada welcomed the Francophone and Commonwealth summits in quick succession, then welcomed the world to the Calgary Olympics February 13-28. At year-end, CSIS and the police were cooperating to prepare for the Economic Summit in Toronto. It is a tribute to the dedication and professionalism of the men and women of CSIS at all levels that the year was without serious security incident.

We welcome the Solicitor General's initiative in launching a series of addresses describing CSIS's work and pointing up, in some detail, its importance to Canadians. Security considerations make it hard for CSIS to blow its own horn. Our perspective, by statute, is one of reasoned skepticism, so it is very appropriate for the Solicitor General to fill the public relations gap.

Our Responsibility

For our part, we believe that Parliament and the public expect the Security Intelligence Review Committee to have strong opinions and to state them clearly in its annual and special reports.

Our objective has been to be fair. Our special report on the so-called Boivin affair* makes the point. We found much that we did not like during the investigation we carried out after allegations were made that a union official, Marc-André Boivin, facing bomb-related charges was a CSIS informant, perhaps even an *agent provocateur*. We learned, for example, that CSIS had retained information originally gathered by the RCMP on trade unions and had not yet reviewed it in relation to the "strictly necessary" retention requirements of the *Act.* In our view, this was out of line with the *CSIS Act.* We were disturbed to find that the *Sûreté du Québec* was not alerted for two days after Mr. Boivin told his CSIS handler that specific and serious criminal offences might be imminent.

But we found that Mr. Boivin was not asked to, nor did he, report to CSIS on union affairs as such; his beat was "subversive" elements. Nor was there any evidence that CSIS ever directed or encouraged him to influence union business or to carry out illegal acts. He was not an *agent provocateur*. As far as targeting and tasking are concerned, CSIS was clean and we said so.

We intend to keep doing business as usual, advising Parliament and the public of the facts as we see them. That is the business Parliament gave us to do. Our hope is that the changes taking place in the way CSIS goes about its business will narrow our scope for criticism.

Business Not as Usual

As a matter of fact, the thread that ties together many of the problems we have flagged was a business-as-usual approach within the Service. We do not suggest an overt and conscious defiance of Parliament's decision in 1984 to change the approach to security intelligence. But CSIS often seemed to lack the will to adjust.

Perhaps that was unavoidable under the circumstances. It seems clear in retrospect that the dislocations of separation from the RCMP were underestimated--even at a material level: four years later, CSIS still does not have a proper headquarters of its own, for example; hundreds of CSIS officers still go to work every morning at RCMP headquarters on Alta Vista Drive in Ottawa.

In any case, during the first three years, the unquestioned need to keep security intelligence operations rolling was accepted by too many people at all levels as a reason--if not an excuse--to put off such matters as bringing files inherited from the RCMP into line with new statutory requirements, moving towards an acceptable level of official bilingualism, and aggressively searching out recruits with the research and policy backgrounds needed to do modern security intelligence work.

While 1987-88 has been a difficult time for CSIS, it has surely laid to rest any expectation that business can continue as usual. We have chosen the familiar expression "turning the

---

* *Section 54 Report to the Solicitor General of Canada on CSIS' Use of its Investigative Powers with Respect io the Labour Movement,* made public by the Solicitor General on March 29, 1988 (see Chapter 3 below for a fuller description of our findings and conclusions).

corner" for the epigraph of this year's Annual Report. Readers will find that we still have many criticisms, but we believe that CSIS is on the right road.

2. Oversight

Under the *CSIS Act*, the Security Intelligence Review Committee (SIRC) is Parliament's and the public's watchdog on the Service. Our mandate as a Committee is to see that CSIS carries out its work effectively, on the one hand, but without unreasonable or unnecessary intrusion on individual rights, on the other. Specific tasks assigned us by the *Act* fall into two broad categories--oversight and complaints. We also have a statutory obligation to report on our work once a year. In this, our Annual Report, we describe our work as fully as we can within the limits imposed by the need to protect national security.

Chapter 8 of this Report deals with the complaints process. In this chapter and the five that follow we report on our oversight activities under sections 38, 40 and 54 of the *Act*. Paragraph 38(a) directs us "to review generally the performance by the Service of its duties and functions" and lists a series of specific tasks. Paragraph 38(b) and section 40 provide for reviews aimed at "ensuring that the activities of the Service are carried out in accordance with this *Act*, [and] the regulations and directions issued by the Minister ... and that the[se] activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers". Under section 54, we may make special reports to the Solicitor General.

Because of its wide powers of investigation and the secrecy that unavoidably surrounds much of its work, CSIS comes under a number of controls. It can use its most intrusive powers--opening mail and tapping telephones, for example--only if it has warrants from the Federal Court of Canada. Each application for a warrant requires the personal approval of the Solicitor General. The Solicitor General has other controls as well. Formal agreements with provinces to ensure CSIS access to information held by police require his personal approval, and he issues formal instructions on the conduct of cases and entire classes of case. The Solicitor General has his own watchdog on CSIS, the Inspector General. Our oversight mandate extends to CSIS compliance with all of these controls.

Warrants

We expressed a number of concerns in last year's Annual Report about the targeting and warrant processes. As a result of the "mid-course correction" unveiled by the Solicitor General on November 30, 1987, CSIS has gone a very long way to meeting our concerns. The new arrangements are reviewed in Chapter 3 of this Report. The outstanding issues of solicitor-client privilege and emergency warrants, which may call for amendments to the *Act*, are dealt with in Chapter 10.

Ministerial Instructions

The 1987-88 ministerial directives we received are listed in Appendix A of this Report. After carefully examining 13 of them, we are of the opinion that they do not permit any unreasonable or unnecessary use of the Service's powers, nor do they impinge unduly on individual rights or privacy. In fact, most tend to circumscribe the independent authority of the Service and increase accountability to the Solicitor General. The same is true of two 1986-87 directives that arrived too late for us to review in our last Annual Report. Six 1987-88 directives arrived too late to be examined before this Report went to the press.

As promised (Annual Report 1986-87, page 6), we have begun to compile statistics on operations requiring ministerial approval. While security considerations prevent us from revealing the details of any operations, we can say they are very few in number.

In 1986-87 we discovered that we were not routinely getting copies of some documents we would consider ministerial directives or direction (Annual Report 1986-87, page 6) because of a narrow interpretation given to subsection 6(2) of the *CSIS Act*. The Department of the Solicitor General is in the process of developing criteria to ensure that we will be provided with everything properly falling under subsection 6(2). This process will be completed soon.

However, we discovered a new twist this year. In a news release dated February 25, 1988, the Solicitor General announced "new ministerial controls over CSIS investigations". (They provide that CSIS must have the Solicitor General's personal authority to conduct any intrusive investigation whatsoever in counter-subversion cases.) We found that these "new controls", while not the subject of formal written communications to CSIS by the Solicitor General, took the form of amendments to CSIS's Operational Manual.

The Manual is a compendium of step-by-step rules for CSIS employees. It is prepared by and is the responsibility of CSIS. It includes all ministerial instructions, of course. At many points it elaborates on these instructions in minute detail, prescribing forms to be used and lines of authority to be followed.

In accordance with subsection 7(l) of the *Act*, CSIS consults with the Deputy Solicitor General concerning general operational policies. In fact, the Deputy Solicitor General is consulted when the Manual is amended. We will henceforth give the same attention to changes in the Manual as to ministerial instructions under subsection 6(2) as they appear, in practice, to have equal standing.

Agreements with Other Organizations

Copies of nine new CSIS agreements with other organizations in Canada and one with a foreign agency were passed to us in 1987-88. We were satisfied with them as far as they went, but they raise two issues.

One is the completion of CSIS's arrangements with provinces for exchanges of information with police forces and for mutual assistance. Three of the nine domestic agreements signed last year are in this category. With the conclusion of an agreement with Manitoba soon after the end of the year under review, CSIS had agreements with all but one province--Quebec. The absence of a formal agreement does not by itself indicate a lack of cooperation that could compromise national security. But we are of the view that formal agreements are useful as an exercise in setting guidelines, so everyone knows what is permitted and, equally important, what is not.

The other issue is control over the transfer of personal information in the Service's hands. Most of the Service's agreements with departments and agencies of the federal government (which accounted, incidentally, for the other six domestic agreements we saw last year) cover the provision of information to CSIS under the terms of the *Privacy Act*. No exception can be taken to this.

But the CSIS management information system has not permitted easy identification of information and intelligence passed to other agencies. This effectively prevents us--short of making manual searches that would exhaust an army of researchers--from carrying out our statutory duty under subparagraph 38(a)(iii) of the *CSIS Act* to "monitor the provision of information and intelligence pursuant to those arrangements" with other agencies, both domestic and foreign.

We should say that the ongoing sampling we do has revealed no exchanges of information that we take exception to; information provided to others about residents of Canada was within the terms of the relevant agreements. Information exchanged under most of the relevant agreements is for visa vetting and security clearances.

However, we expect that a projected overhaul of the Service's computerized management information system will introduce programming that will permit easy access to data on information about Canadian residents exchanged by CSIS and other agencies (see Annual Report 1986-87, page 39). CSIS needs to be more attentive in general to keeping records of its activities, for the sake of its own monitoring as well as ours. And we wish to see a specific policy, guidelines and auditing procedure developed for the release of any information on a Canadian resident.

One bit of unfinished business (Annual Report 1986-87, page 18) was cleared away in 1987-88. CSIS prepared, at our request, a new descriptive catalogue of its arrangements with police and intelligence agencies in other countries. It was a considerable improvement over the incomplete list we were handed in 1985. After making inquiries about the nature of the agreements with 11 agencies in as many countries, we are satisfied that CSIS now has an up-to-date list of its international arrangements.

Disclosures in the Public Interest

Paragraph 19(2)(d) of the *Act* authorizes certain disclosures to public servants and to ministers other than the Solicitor General, the Secretary of State for External Affairs and the Minister of National Defence. Subsection 19(3) requires the Director to report such disclosures to us. None was reported in 1987-88.

In this connection, we have (Annual Report 1986-87, page 30) previously expressed concern that the *Act* makes no provision for warning individual Canadians when they are drawn into the orbit of front organizations that covertly serve purposes or foreign governments inimical to Canada's national security. If we do not expand on this theme here it is only because it is covered this year in Chapter 10, our look ahead to the five-year review of the *Act*.

Unlawful Acts

Two reports were given to us under section 20 of the *Act*. This section requires the Director of CSIS to advise the Solicitor General when it appears that an employee may have acted unlawfully in the course of duty. If the Solicitor General passes such a report on to the Attorney General of Canada, we get a copy together with any comments by the Solicitor General. In one case no charges were laid. In the second, the Attorney General

referred the matter to provincial authorities, which had not decided by year-end whether to lay charges. In both cases, we are satisfied that CSIS management is being strict in protecting the public from illegal acts that might be committed under the cloak of the *CSIS Act.*

CSIS Annual Report and Certificate of the Inspector General

Section 33 of the *CSIS Act* provides for an annual report to the Solicitor General by the Director of CSIS and for a certificate to be issued by the Inspector General saying whether the report is satisfactory--in particular whether the Service has done anything not authorized by the *Act*, anything in contravention of any instructions issued by the Solicitor General or anything that involves an unreasonable or unnecessary use by the Service of its powers. Section 33 further provides for the transmission of the Director's annual report and the Inspector General's certificate to us.

We are unable in this Report to comment on the 1987 certificate of the Inspector General, as there was no Inspector General at the time to issue one. Dr. Richard Gosse, who filled this office with distinction from its inauguration in 1984, left in February to become the first chairman of the Public Complaints Commission for the RCMP, and he had not been replaced by fiscal year-end. We take this occasion to thank Dr. Gosse for the cooperation he extended to us. We found that we could rely on his office to be thorough and industrious in the fact-finding it did on our behalf, as provided for in section 40 of the *Act*. He established a high mark for his successor to reach.

Statistics on Operational Activities

Subparagraph 38(a)(viii) of the *Act* gives us an explicit mandate "to compile and analyse statistics on the operational activities of the Service". We continue to compile and analyse statistics in a number of areas--the use of intrusive investigative techniques (e.g., the number of wiretaps authorized by warrants), the flow and retention of information (e.g., file retention; see page 14), and investigative levels (e.g., the number of field investigations in connection with security screening; see page 19).

CSIS meets with us at the drafting stage to discuss the eight to ten statistical papers we prepare each year. As a result, we reach our interpretations of the statistics in full knowledge of CSIS's interpretations, and these meetings are a useful learning experience for us.

Special Studies

We made two special reports to the Solicitor General under section 54 of the *Act* in 1987-88. One was on CSIS's use of its investigative powers with respect to the labour movement. As indicated in Chapter 1 above, it was made public by the Solicitor General on March 29, 1988. We discuss some of our findings in Chapter 3, below.

The other report was on security screening in immigration matters. The Solicitor General did not publish it because he believed that it contained sensitive national security information. But he noted in his response to us that it raised many important concerns, and it is

being used in an interdepartmental study prompted by recommendations made by the Standing Committee of the House of Commons on Labour, Employment and Immigration in its report of June 17, 1986.

Also, as we promised last year, we started a review of the system for safeguarding scientific and technological assets in Canada, relying primarily on structured interviews with federal officials involved in this area. We met with people from the Privy Council Office, Revenue Canada (Customs), the Department of External Affairs, the Department of National Defence, Supply and Services Canada and the RCMP, as well as with CSIS officials. Because of the large number of players in this field, the analysis and consultations leading to the final report are not yet completed.

We are pursuing a program of studies that will let us complete a comprehensive review of the basic functions of the Service by the time our mandate expires in 1989. In 1986-87 we reviewed the counter-subversion program, which raised serious questions about targeting--that is, the way CSIS selects subjects for investigation (see Chapter 3 of this Report for an update). This year we zeroed in on the counter-terrorism program (see Chapter 5) and intelligence assessment (Chapter 6). In the coming year, we will turn our attentions to the counter-intelligence program and CSIS investigations, if any, of the peace movement in Canada.

In carrying out these major studies, we have developed the practice of working out detailed terms of reference with the responsible CSIS managers. Thus they fully understand what information we need and can direct us to the appropriate files and documents. The Service, for its part, has developed the practice of designating a member from the unit under study to provide liaison. This officer works with us to manage the study in such a way that it interferes as little as possible with ongoing operational responsibilities.

Budgeting Information

We get the update of the Multi-year Operational Plan (MYOP) that CSIS, like all arms of the federal government, carries out annually. We recognize that the information in the Service's 1987 update meets Treasury Board's requirements. But it does not alone give us the bird's-eye view that we want to have of CSIS as an organization. It does not let us answer the question, does CSIS have the money and personnel it needs?

We should say that we have no evidence from the available information that CSIS is being spoiled by excess funding or staffing. If anything--and despite a sharply rising budget--we suspect that it is being asked to spread itself rather thin.

But we have now asked the Service for detailed corporate financial and human resources information. In particular, we have asked for a reconciliation of the MYOP data with data found in the Main Estimates, year-end audited financial statements such as those found for other agencies in the Public Accounts of Canada, and detailed information on the allocation of person years among various functions. We hope to complete a review of CSIS's resources and how it uses them before the end of our mandate.

Consultations

In our oversight role, we also have dozens of routine consultations. We meet the Solicitor General quarterly as a group, and our Chairman meets him monthly as well as occasionally meeting with the Deputy Solicitor General. The Chairman also meets regularly with the Director of CSIS. Both the full Committee and the Chairman meet occasionally with the Inspector General, and there are frequent meetings between the Inspector General and our Executive Secretary. In the past year, there were also meetings with the Independent Advisory Team created by the Solicitor General to follow up concerns we had expressed in past reports.

In 1987-88 we continued our practice of visiting regional and district offices of the Service rather than confining our contacts to Headquarters in Ottawa. This allows us to be briefed on regional operations by the people most in the know. We usually hold separate meetings with regional or district managers and with the rank and file so we can engage in frank exchanges in which we hear the concerns of people in the field and answer questions about our own role. CSIS has been very cooperative in this program. During the year under review we visited four regional and district offices--in Winnipeg, Vancouver, Montreal and Toronto. In the coming year, we will visit the Halifax and Quebec City offices as well as making return calls at Vancouver and Toronto.

Further afield, we made a tour of Hong Kong, Australia and New Zealand in November, 1987. In Hong Kong, we focused on the work done there to keep abreast of a flood of immigration requests. The number of immigration files originating in Hong Kong is about 25,000 a year and growing as people and money seek safe havens in anticipation of the takeover by China in 1997. What we learned there was of material help to us as we prepared our special report on security screening in immigration.

Australia and New Zealand are of particular interest as two countries with which Canada enjoys excellent relations. In addition, Australia's complaints process is close to ours--closer than that of any other country. What we learned there informs a number of our observations in this Annual Report.

Inquiries and Briefings

With the sole exception of cabinet confidences, we have access to all information in CSIS's hands. Last year we directed 95 written inquiries to the Service and had answers to 85 by year-end. That left a total of 10 questions unanswered at that time; of these, four were put to the Service in the last month of the fiscal year. As provided for in the *CSIS Act*, we sometimes have our fact-finding done by the office of the Inspector General. In 1987-88, the office of the Inspector General carried out three reviews of specific activities of the Service for us.

We also get briefings from CSIS on particular matters. Two that are of great public concern are the Air India disaster and the Narita Airport explosion, on which we received monthly updating in 1987-88. We have already, in Chapter 1 above, dealt with some allegations that have been made in the media. With regard to the erasure of tapes, it would be most improper

for the Service to let wiretap tapes accumulate indefinitely in case they might eventually prove useful to the police. CSIS's job is to collect *intelligence*. Wiretap tapes commonly include a great deal of personal and other information that does not belong in secret files. We believe CSIS is correct when it notes the pertinent information that its wiretaps provide, then destroys the tapes.

Beyond that, it is not for us to add to the public record on the Air India tragedy. We are deeply conscious of the frustration felt by Canadians that no charges have been laid three years later. The RCMP continues its investigation, and CSIS's role at the moment is to provide it with security intelligence assistance.* We will continue to monitor developments closely.

We also had briefings on the "Atwal warrant affair". The broad lines of this matter are on the public record as the result of proceedings in the Federal Court of Canada. What is perhaps not well understood is that the Service did not deliberately "cook" its warrant application by including information from a discredited source. When the affidavit was first drafted, the information was considered reliable. Only after the paperwork had moved to CSIS Headquarters did the regional office concerned decide that the source could not be trusted. The failure occurred when Headquarters was not notified. That is a serious matter, but it is not deliberate falsification. We believe that new procedures described in Chapter 3 improve the safeguards against lapses of this kind.

In another matter that came to public attention during the year, we satisfied ourselves that CSIS dealt properly with Ryszard Paszkowski, who went to the media in January, 1988, with a complex account of how his work for CSIS let him in for a year in a West German jail to complete a hijacking sentence. As the Solicitor General has confirmed in the House of Commons,** Paszkowski did work for CSIS after entering Canada illegally, but CSIS did not bring him into the country to be a double agent, as he claims, and it ended the relationship before Paszkowski voluntarily left Canada in August, 1986, and went to Italy, whence he was extradited by West Germany.

Our Relations with CSIS

Our relations with CSIS continue to be at arm's length. This is as it should be. We share an ultimate goal--effective security intelligence within the limits imposed by the values of a free and democratic society. But our roles are different and, to the extent we are both doing our job, they inevitably bring us into opposition at times.

In general, our reading is that CSIS plays by the book in dealing with us. In the oversight area, relations are at least correct. Often they are cordial. We have already noted in this chapter that CSIS has been very cooperative in arranging our visits to its regional offices and has put no obstacle in the way of our meetings with the rank and file separately from regional

---

* In the case of the Narita Airport explosion, legal proceedings are underway. The British police arrested a suspect in England on February 5, 1988. On August 9, 1988, the Magistrate in London ordered Inderjit Singh Reyat extradited to Canada to face charges, including two counts of manslaughter for the deaths at Narita. As this Report was going to press, the defendant had filed an appeal to that order.

** *Debates of the House of Commons,* January 22, 1988.

management. When we investigate specific complaints, relations are more distant and formal. That is also proper, because then we are acting in a quasi-judicial capacity.

We can well understand some wariness on the part of the Service; although we reject any suggestion that our exercise of review and investigative powers affects the Service adversely. Oversight in one form or another is becoming the common experience of Western intelligence agencies, but Australia is the only other country we know of where an independent body* has unrestricted access to security intelligence files.

We like to think of our relations with the Service in terms of creative tension. Although our reports are often critical of systems--the nature of our mandate ensures that they often will be--we want to express again our respect and admiration for the people who work for the Service. They have a difficult role in which, as it has often been observed, the successes must remain secret while the inevitable failures always seem to become known.

---

* The Inspector General.

3. CSIS Operations

The essence of CSIS's mandate is spelled out in section 12 of the *CSIS Act*. It says that CSIS "shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada".

"Threats to the security of Canada,, are defined in section 2. They fall into four categories--espionage or sabotage, foreign interference in Canadian affairs, the use of violence to gain political ends in Canada or another country and, fourth, covert or potentially violent attempts to overthrow our constitutionally established system of government. "Lawful advocacy, protest or dissent" are explicitly excluded unless they are carried on in conjunction with any of the threats spelled out in section 2.

In Chapter 2 we dealt with controls on the Service's use of its powers in carrying out its mandate. This chapter and the three that follow review operational matters--how CSIS guards the security of Canada.

Counter-subversion Operations

In line with a recommendation in our last Annual Report (page 40), the counter-subversion arm of CSIS was disbanded in November, 1987, and its responsibilities were reassigned. As a result, CSIS investigation of home-grown threats to national security now better reflects their modest scale. It better reflects, too, the "strictly necessary" limit set out in section 12. Cases of suspected foreign activity inimical to Canada's interest are now handled by the Counter-intelligence Branch, while cases in which there appears to be a real risk of violence are handled by the Counter-terrorism Branch.

A residue of counter-subversion targets are now monitored by the Analysis and Production Branch, which adds to the files any relevant information that comes its way in the media or as a spin-off from other inquiries in order to provide the Government with what the Solicitor General has called "a watching brief".* But the Operational Manual has been amended so any active investigation of these cases in future will require the Solicitor General's personal authorization. We believe this is a good control; the initiative remains in CSIS's hands, sheltered from considerations of partisan political expediency, yet there is political accountability when an initiative is followed through.

In total, slightly more than 3,000 of the files that had been actively pursued in the counter-subversion program remain open. But only a small percentage of these are now under active investigation by the Counter-terrorism or Counter-intelligence Branches, the rest are only being monitored.

After examining targeting and the use of intrusive powers, we can affirm that from the time of the Solicitor General's announcement to year-end no group was subject to investigation solely under paragraph 2(d) of the Act--the "counter-subversion" provision.

---

* Solicitor General of Canada, Notes for an Address to the Conference on Advocacy, Protest and Dissent, Queen's University, February 25, 1988.

Fall-out 1: Files

Controversy over the fate of the counter-subversion program brought to light much more factual information than had previously been available on the extent of the Service's stock of information on individual Canadians. In our last Annual Report (page 38), we said that the counter-subversion branch "probably [had] more than 30,000 files on individuals--how many more, no one knows". Now we do know, and our figure turns out to have been as conservative as we expected. The Service subsequently did the necessary research and turned up about 54,000 such files.

In the same passage, we said that only a small proportion of the people with counter-subversion files were under active investigation, but we did not reveal how many as this was classified information. CSIS subsequently told the media that the number was 3,867.

The vast majority of counter-subversion files already inactive a year ago have now been locked away pending review. These include all files on labour organizations. With the end of the moratorium on the destruction of files, many of these files should soon be on their way to the shredder, others to the closed collection of the Public Archives of Canada.

We also expressed concern in last year's Annual Report (pages 21-23) about material that CSIS inherited from the RCMP Security Service, including most of the counter-subversion files. We thought it likely that much of this material failed the "strictly necessary" test and did not relate to "threats to the security of Canada" as defined in section 2. In addition, we noted that because of the moratorium, tens of thousands of files that had outlived their usefulness were still on hand.

We do not quarrel with the moratorium as such. It was imposed in February, 1985, after the Deschênes Commission on war criminals found that some immigration files it needed had been routinely destroyed years before. In any case, now that it has been lifted a unit has been set up within CSIS to review files and designate those that are to be destroyed. Some 67,000 intelligence files slated for destruction by the RCMP, before the creation of CSIS, have already been destroyed. We will continue to monitor progress.

As to the retention in active files of information that was originally gathered by the RCMP and may not meet the tests of section 2 and section 12, CSIS has now started a review aimed at weeding out information that should not be there. We recognize that it will take years to go through all the files. We will also monitor progress in this exercise.

Furthermore, starting in January, 1988, no information can be placed on these files unless the subjects fall under new and tighter targeting procedures described below. In line with our recommendation (Annual Report 1986-87, page 38), detailed criteria that satisfy us have been developed for opening files on individuals and groups.

Fall-out 2: Targeting and Warrants

There has been action on a number of other issues we raised last year in the context of the counter-subversion study. CSIS has established a task force to review all policy and it is overhauling its Operational Manual to bring it into line with the *CSIS Act.*

With respect to warrants, change was hastened by the revelation last November that information from a discredited source had been left in a successful application before the Federal Court for authority to intercept telephone communications in a counter-terrorism investigation. Both CSIS and the Inspector General launched thorough reviews of warrants then in effect. In particular, the Service set about verifying and documenting every allegation of fact contained in warrant applications. We intend to review this exercise.

More important for the future, a number of measures were taken to improve accountability. Warrant coordinators ensure that all relevant policies and procedures have been respected when an application is made. All facts set out in the affidavits underwriting applications are documented. A new Affidavit Content Certificate places explicit responsibility on the four people who sign it. An analyst and unit head certify that the facts alleged are backed up by the CSIS data base. A chief attests to the reliability of the reports from which the facts were drawn and to the need for the powers requested. A director general certifies that the information required by subsection 21(2) of the *Act* has been provided.

Warrant applications now also include more discussion of the powers to be used. When a renewal is sought, the analyst reviews the information already obtained through the use of powers authorized by the warrant. If nothing useful was turned up, alternative investigative techniques must be considered.

The procedure for targeting has also been improved. Mirroring the warrant process, facts cited in any proposal to target an individual (a "Subject Evaluation Report" or SER) must be documented, and opinions and recommendations must be distinguished from the facts. A "complete and balanced description" of the proposed target's activities must be provided. We had urged (Annual Report 1986-87, page 38) that SERs "rely less on isolated incidents and more on coherent argument for the targeting decision that TARC [the Target Approval and Review Committee] is asked to make".

The consequences to national security if the powers concerned are not granted--in other words, the real need for the warrant--must also now be considered. The revised Operational Manual places a duty on investigators to ensure that the use of intrusive techniques is weighed against possible damage to constitutional rights and freedoms. As in the warrant process, when authorization of an investigation expires, an investigator seeking renewal must provide an Assessment Report, which turns the spotlight on whether there have been any changes in the initial assumptions--whether the target is still capable of carrying out its aims, for example.

There have been positive changes in the treatment of groups in accordance with recommendations made in our 1986-87 Annual Report. Investigation of people we have termed second-stage targets"--those who come to CSIS's attention only because they are in contact with primary targets (Annual Report 1986-87, page 36)--is limited to identifying them.

Both TARC and the Warrant Review Committee now sit under the personal chairmanship of the Director, and the Warrant Review Committee includes a Justice Department lawyer to act as "devil's advocate", challenging the need for each warrant in the first place. In line with a recommendation we made in last year's Annual Report (page 38), a centralized index of all targets is maintained.

A remaining reservation is with the level at which the devil's advocate participates in the warrant application process. When we made this proposal in the first place (Annual Report 1986-87, page 9), we suggested that this official intervene before the Solicitor General or the Federal Court itself. We feel that the situation where the devil's advocate is a minority of one, outnumbered by other officials on the Warrant Review Committee, has not yet gone quite far enough. However, we understand that the proper role for the devil's advocate is currently under active consideration.

It remains to be seen how well the new procedures are respected in practice. But they certainly go a long way towards meeting many of the concerns we have expressed in the past (Annual Report 1986-87, pages 36-38). Early indications are encouraging. We have looked at some of the post-reform warrant applications, and we are initially satisfied with the change that has taken place. Compared with what we had seen before, they are models of precision, clarity and logic.

A Case in Point

The "Boivin affair" illustrates some of the concerns we have had--and some of the work CSIS had already done, before the recent flurry of changes, to bring its targeting practices into line with the *CSIS Act*.

This affair erupted when the media reported that Marc-André Boivin, an official of the Confederation of National Trade Unions (CNTU) facing bomb-related charges in the Quebec courts, was a CSIS source, perhaps an *agent provocateur* whose illegal activities were part of a CSIS plot to disrupt and discredit the labour movement. Using information gathered by the Inspector General, we looked into these allegations and the Solicitor General made our report public on March 29, 1988.*

We found that Mr. Boivin became a source for the RCMP in 1973 with instructions to monitor suspected criminal and "subversive" activities in the labour milieu. On two occasions he had brushes with the law in connection with his union work--in 1973 for causing a disturbance while picketing and in 1978 for putting glue in the locks of a public building. The RCMP told him in the 1978 incident that he was not to take initiatives "not in keeping with our policies and the law of the land". By 1983, the RCMP Security Service's labour desk was only monitoring, not investigating.

By the time CSIS took over from the Security Service in 1984, Mr. Boivin was no longer targeted on the labour movement. He was targeted on communists and foreign-influenced agents attempting to influence the labour movement. It is clear from documents and interviews that CSIS took pains to ensure that Mr. Boivin understood the limits on his assignment, that he had no mandate to report on union activities or on the activities of union members except as they directly related to communist or foreign influence.

Indeed, our investigation showed that CSIS has not directed any human source against any union or any individual union members in their union capacities. It also showed that reports

---

* *Section 54 Report to the Solicitor General of Canada on CSIS' use of its Investigative Powers with Respect to the Labour Movement.*

from sources knowledgeable about the labour movement did not include such matters as strike activities, international organization, membership, bargaining positions or general political, economic or social goals.

We were disturbed to learn that CSIS waited two days to inform the *Sûreté du Québec* after Mr. Boivin told it there would be bombing attempts in Drummondville and Montreal. But we found that Mr. Boivin had been given appropriate directions by the Service and that no improper attempts were made to protect him once the charges were laid.

We were also disturbed to find that CSIS still held files put together at a time in the 1970s, before the *CSIS Act*, when the RCMP did investigate unions as such. CSIS had added to these files in line with its normal procedures. Even in the absence of a targeting decision, CSIS researchers routinely posted any information that came their way in the appropriate file if there was one. We also found that these files were fully accessible to CSIS investigators.

The Solicitor General and the Director took action that we consider appropriate. Files on labour unions were locked up and are now awaiting review, and if they do not meet the criteria of the *Act* they will be destroyed or sent to National Archives. Instructions were given that monitoring was to cease where it could not be justified under the *Act*.

Open Sources

CSIS's use of open sources has been one of our continuing concerns. The under-use, rather. By open sources we mean such things as the mass media and scholarly and technical journals, both Canadian and foreign, as an alternative to intrusive investigation. We found, for example, that Australia's ONA draws on information from intelligence sources and also relies heavily on published information, both journalistic and scholarly.

CSIS maintains and adds to open sources in its Information Centre (previously called the Open Information Centre), which provides library and data base search services for CSIS investigations and analysis. But a proclivity for investigative techniques is endemic in CSIS; the Service seems to give more credibility to information it has ferreted out through investigation than to information available to any astute reader.

Our concerns were echoed in the report of the Independent Advisory Team. In one of its few departures from the recommendations we made in our last Annual Report, the Independent Advisory Team did not agree that CSIS researchers should be pursuing independent research or preparing summaries of information on file. But, overall, it supported our view that the Information Centre should be made more relevant to the activities of the intelligence analysts in CSIS. It noted "the Service's apparent hesitancy to exploit open source information to its full potential" and said that "important threat assessments, certainly at the strategic or environmental level, could be completed primarily on the basis of open information".*

---

* Independent Advisory Team on the Canadian Security and Intelligence Service, *People and Process in Transition*, pages 20-21.

There have been some welcome changes since our last report. Holdings of French-language materials have been increased to 28 per cent of the total-a proportion that library specialists we consulted tell us is excellent for a specialized library of this kind. The increase was not solely aimed at meeting a language quota as such but to ensure that the most useful materials available in French were accessible to investigators and analysts working in both official languages.

Year-to-year comparisons of how much access analysts seek to open information through the Information Centre are difficult because of changes in the way the Information Centre records requests for its materials. But it appears that a sharp rise in the use of the Information Centre in 1987 from 1986 resulted from requests by administrative and technical units. Demand from analysts in the operational branches seemed to drop by almost the same amount, even when figures are weighted to take account of the fact that counter-subversion branch statistics were collected for only part of the year. These statistics, however, do not take into account several open source documents which the Information Centre routinely distributes to the operational branches.

The news from the regions is encouraging. Staff is being trained for regional Reference Centres. We are also encouraged to see that there are now Reference Centres in Montreal, the Ottawa regional office and Toronto, all with up-to-date facilities for accessing data, and that others will open soon in Vancouver and Edmonton. With easier access to open information, investigators in the regions have less reason to use intrusive powers.

Warrant Statistics

There was a significant drop in the number of warrants authorized in 1987 (see Table 1). Part of this reduction is accounted for by the elimination of most counter-subversion warrants, part by the introduction of new warrant authorization procedures following difficulties with the Atwal warrant.

Table 1. New and Renewed Warrants Granted to CSIS, 1985 to 1987

	1985	1986	1987
New warrants	82	94	71
Warrants renewed	27	11	5
Total	109	105	76
Average duration of warrants (days)	173.6	162.2	190.82

Source: CSIS

The statistics in Table 1 follow the pattern of each of our previous annual reports. But in each of those reports we said that we wanted to find a way to provide more precise information about warrants without harming national security.

We have tried to achieve this in a variety of ways, but each new idea has been still-born because of CSIS's sincerely held view that to reveal more would give undue assistance to those engaged in espionage or terrorism.

While we disagree with CSIS, we take the Service's objection seriously, based as it is on national security concerns. Accordingly, we will propose a statistical format that we believe would be useful to Canadians when a Parliamentary Committee commences the five-year review of the *CSIS Act*, scheduled for next year. Parliament itself will then decide whether the Act should require the publication of statistics similar to those we will propose, or whether CSIS's national security concerns are sufficiently well-founded to make such action imprudent.

In any event, we can assure Canadians that we will continue to examine all warrants each year, and will immediately inform the Solicitor General and, if necessary, Parliament should there be any misuse, in our opinion, of CSIS powers.

The proposal we will make to the Parliamentary Committee is that the *CSIS Act* require the provision of statistics detailing the number of Canadian citizens or legal permanent residents who have been affected--even marginally--by surveillance powers granted to CSIS under a Federal Court warrant.

Since we believe that to reveal the precise number of non-Canadians affected by warrants could perhaps harm national security, we do not propose to break down the total number of warrants authorized by the Federal Court between those affecting Canadians and those affecting foreigners in Canada. For the same reason, we do not propose to make public the total number of individuals affected by warrants.

In our view, the annual publication of the number of Canadians and legal permanent residents affected by Federal Court warrants granted to CSIS would give the public meaningful information about how CSIS powers were being used, without harming national security. We believe that such statistics would be much more useful than the numbers we have published this year, and would be most unlikely to harm national security. However, we will await Parliament's decision on this issue before making any changes.

Security Screening

The length of time it takes to process applications for security clearances remained a serious problem in 1987-88. It was still taking more than seven months to conduct checks at Levels I (previously called CONFIDENTIAL) and II (SECRET), more than a year at Level III (TOP SECRET). CSIS is the first to recognize that this is too long; it agrees that 30 days would be a reasonable target for clearances at Levels I and IT, and the Committee believes that, ideally, 90 days would be appropriate for Level III.

Why are these targets not being met? The explanation is simple: CSIS is swamped. During the year, it dealt with about 90,000 requests to check on prospective immigrants and another 90,000 for checks on applicants for citizenship, 46,000 under the Government Security Policy (GSP), 14,000 for airport workers and 7,000 in other categories.

As intended when the GSP was introduced in 1986, fewer clearances were required under this heading. Requests fell by more than a third from the 1986-87 level. The number of time-consuming field investigations required was also off by a substantial number.

But any hope that this would ease the pressure on CSIS was scuttled by the Department of Transport program to require clearance for all airport workers with access to restricted areas, as a counter-terrorism measure. It was recognized from the outset that these clearances would have to be spread over several years, starting in 1987-88. The first-year target was 10,000. The estimated number of requests in the first year alone is anticipated to be 24,000 to 28,000. Already stretched thin, CSIS was faced with a demand which was 240 per cent of the expected level.

A short-term complication was a rush of major international events in Canada. Nearly 600 Level II clearances were required for the Commonwealth Heads of Government Meeting in Vancouver October 13-17 and about 500 for the Economic Summit that was coming up in Toronto in mid-June, 1988.

Among other problems, the Security Screening Branch is also a victim of the inadequate physical plant provided for CSIS. Analysts are not housed in the same building as records that they must consult. While computer terminals sit in storage because everyone is too busy to see to their installation, Branch employees line up to use the limited number of terminals already plugged in. Many positions in the Branch are vacant.

It is not surprising that, despite the provision of additional resources, a mountainous backlog remained--43,000 citizenship clearances, 33,000 immigration clearances and 15,000 clearances under the GSP. Recognizing that the situation was out of hand, CSIS called in an expert from Treasury Board to see how the system could be streamlined and what further resources were needed. The recommendations contained in the expert's comprehensive report are being implemented and CSIS has shown creativity and flexibility and, indeed, has come up with further improvements to supplement those contained in the report.

An important change is that CSIS's responsibilities in citizenship screening are being streamlined and this will provide a more cost-effective use of Security Screening Branch resources as citizenship accounted for a third of all clearance requests.

CSIS anticipated that by the middle of July, 1988, the entire backlog--including all screening-will be 35,000-40,000 in total, less than half of what it was six months before.

4. Inside CSIS

Our last Annual Report and our special report on staff relations and language issues in CSIS, *Closing the Gaps*, followed by the report of the Solicitor General's Independent Advisory Team ... all had a major impact last year on the way CSIS conducts its internal affairs. It was not an easy year for the Service, but we see considerable improvements that will make things easier in future. Highlights are discussed in this chapter.

The Academy Revisited

We were encouraged by the decision to reopen the Sir William Stephenson Academy in April, 1988. The Academy is CSIS's own school for training new Intelligence Officers (IOs); it is the doorway through which a new generation is entering the security intelligence field.

We had been deeply disappointed to learn in the spring of 1987 that the Academy would shut its doors for a year. After spending a great deal of money by hiring a large group of intelligence officers at the IO-3 level in autumn, 1986, CSIS said it could not afford to put a class at the lower IO-1 level through the Academy in the 1987-88 fiscal year. What bothered us was that almost all the autumn, 1986, newcomers were ex-police-officers. Entering at a more senior level than Academy-trained recruits from civilian life, they would be in line for faster promotion. It appeared to us that CSIS was missing a chance to diversify the mix of experience and background in its staff.

But in 1987-88, CSIS kept a commitment to stop hiring IOs this way. The only new employees who did not come in through the Academy were middle or senior managers with specific expertise that the Service needed. At the same time, plans were made to provide early retirement for some long-serving officers, which will make room for more new blood.

As to the Academy program as such, we have always been enthusiastic. While much of the transition process, as CSIS took over from the RCMP Security Service, was marked by turmoil and delay, we said in our Annual Report for 1985-86 that "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". CSIS reaches beyond the security and intelligence community for lecturers at the Academy, into the universities and the Canadian Civil Liberties Association. At year-end, one of our number, Jean Jacques Blais, was scheduled to address the April, 1988 class on our role as a Committee.

Representation and Bilingualism

As the year ended, the April, 1988 class had been assembled. With 12 members, it was very small--the smallest class ever. But it is a step forward, nonetheless. Making the Service more representative of the society it serves is an important objective in recruitment. We find the composition of this class reassuring (Table 2).

With respect to language and sex, these proportions are not as lopsided as they may appear at first glance. They are what CSIS needs if it is to become more representative of the Canadian people. As one of our number, Paule Gauthier, remarked in an address to the Association of Federal Women Lawyers on January 13, 1988, "the realm of national security is not one where women are much in evidence. History tells us of women who have carried off prodigies of spying, but the number of women in leadership roles at the Service is minimal, if not negligible".

Table 2. Composition of classes at the Sir William Stephenson Academy

Starting Date	Sex		First official language		Source	
	M	F	E	F	Outside	Conversion
Jan 1986	25	8	32	1	33	0
Feb 1986	9	5	8	6	0	14
Jun 1986	16	4	18	2	20	0
Sept 1987	5	2	3	4	0	7
Feb 1987	18	2	14	6	20	0
Apr 1988	4	8	6	6	9	3

Source: CSIS

With respect to first official languages, CSIS also has ground to make up in ensuring that it can operate effectively in both English and French as well as ensuring that it is representative of the Canadian people. We are glad to be able to report that the entire class is bilingual.

With respect to the "source" category in Table 2, the nine recruited from outside the Service are recent university graduates. The remaining three are CSIS surveillance officers "converted" to the IO stream. We have already commented in detail (*Closing the Gaps*, Chapter 15; Annual Report 1986-87, pages 52-53) on the morale problem among surveillance officers--the people who stalk CSIS targets--because their work does not ordinarily lead to promotion. We think it is appropriate that CSIS provide reasonable opportunities for surveillants with the appropriate talents to enter the IO category, with its greater opportunities for advancement.

The representation of ethnic and visible minorities and of native peoples is something that still needs to be seen to. We believe adequate representation of these groups is crucial. It is important that they see CSIS as an environment in which they and their values are respected. And CSIS needs the insights they can bring on the reality of today's multicultural, multiracial Canada. Reliable statistical information on ethnicity is always hard to come by. But casual observation provides ample evidence that ethnic and racial minorities and native peoples are underrepresented in CSIS. Clearly the objective should be to achieve more equitable representation.

We note that the RCMP has created a national recruitment team that, in the words of a March 28, 1988, statement by the Solicitor General, "is carrying the message to minority

and native communities that the RCMP is interested in them for a career in law enforcement". There was already an RCMP campaign to attract francophones and women. The circumstances of the RCMP and CSIS are very different, of course; this is a point we often make ourselves. But we note with interest the RCMP's decision to go out to the people it wants rather than wait for them to come to it. We also note with interest the target of five per cent visible minority representation in the RCMP.

Polygraph Testing: From Bad to What?

The news on another of our recurrent themes gives us some concern. We have repeatedly objected to the use of polygraph examinations within CSIS (Annual Report 1986-87, page 46; Annual Report 1985-86, page 15). We will not repeat our argument in detail here. It is enough to say that even supporters of polygraph testing admit an error rate of at least 10 per cent. The polygraph machine registers the physical manifestations of any kind of emotion; it registers fear or annoyance in exactly the same way as it registers guilt. The “result” of the test is an estimate by an operator who interprets what the machine registers. At best the operator makes an educated guess, at worst a shot in the dark.

We do not necessarily believe that the margin of error is only 10 per cent. But we are prepared to argue on that basis and observe that a one-in-10 error rate would be considered very high in most activities. It is too high to justify the mantle of science that polygraph testing can wrap around arbitrary and damaging decisions about the careers of loyal Canadians.

Last year we were pleased to report that polygraph tests were no longer given as a matter of course to people already on the CSIS staff. But there has been one other improvement in the situation since then. Prospective recruits are now put through polygraph tests for loyalty only. They are no longer given polygraph tests on their lifestyle.

Defenders of these tests make much of the fact that polygraph examination is only one of a battery of screening procedures faced by prospective recruits. True enough. But we do not swallow the claim that an unfavourable polygraph reading is ignored when it is contradicted by evidence from other sources. This does not square with our understanding of human nature in the 20th century, steeped in the belief that "science has the answers". It would be difficult to the point of impossibility for the people responsible for recruitment, with the best will in the world, to give a recruit credit for loyalty to Canada when there is an apparently scientific machine saying something different.

Beyond the damage done to budding careers in security intelligence and the blot left on the record of those who "fail" the test, a larger issue looms. If CSIS and its masters in government see the polygraph as reliable enough for use in the recruitment process, how long will it be until they start using it more widely? Can its use in security clearance investigations be far off? Would the private sector long lag behind government? How long until polygraph examinations were routine for millions of Canadians? That is not the kind of society CSIS was created to protect.

We urged "a thorough and objective study ... so the Solicitor General and the Government [could] determine for themselves whether such methods [were] compatible with the values of our free and democratic society" (Annual Report 1986-87, page 48).

An interdepartmental committee pursued this issue in 1987-88. It commissioned a review of current research on the matter, prepared by an independent consultant. So far so good. Unfortunately the review shows unmistakable signs of the haste with which we understand it was assembled. It makes no reference at all to the findings of an important Royal Commission in Ontario* that specifically addressed the matter of polygraph testing in the workplace and only passing reference to testimony on 1983 Ontario legislation that bans polygraph testing for screening personnel.**

While the consultant reviews both the pros and cons and does not explicitly arrive at any strong conclusion, we question the objectivity of a report that refers to polygraph examinations as "a form of psychological testing". As a claim to scientific reliability, this description falls on its face when you consider that the people who administer polygraph examinations are not required to be trained psychologists. In fact, CSIS does use trained psychologists to administer its polygraph tests. But the use of trained psychologists is not a universally acknowledged norm that other polygraph users, in or out of government, could be expected to meet as a matter of course.

On the basis of expertise available to us, we take issue with the description of polygraph examinations as "a form of psychological testing" when its procedures lack validity, reliability and comparability and when the meaning of an individual's reactions is assessed on the basis of a procedure that typically lasts only about two hours.

As 1987-88 closed, events seemed to be racing towards a conclusion. The interdepartmental committee had received a report from a working group and outlined options in a paper for the deputy-minister-level Interdepartmental Committee on Security and Intelligence (ICSI). We have not seen either of these documents (they fall outside our oversight mandate). But we hope that ICSI will not reach any decisions whose roots lie solely in the consultant's report, which we have seen and consider inadequate. We hope that ICSI will make further inquiries--in particular that experts in statistical epidemiology will be consulted.

Management

A number of changes have been instituted in the management of CSIS. The Director's office now includes a Secretariat responsible for planning and coordination and for SIRC and Inspector General Liaison, Ministerial and House Liaison, Committee Organization and Support, and TARC. The Director personally chairs all key internal management committees.

One of these is a new Human Resources Management Committee. The personnel function, including official languages matters, is now headed by a full Deputy Director rather than by a Director General, and we are assured that a comprehensive human resources plan is being developed, covering training and professional development, official languages and recruitment objectives.

---

* Mr. Justice Donald Morand, *Report of the Royal Commission into Metropolitan* Toronto *Police Practices* (Toronto, 1976).

** *An Act to Amend the Employment Standards Act,* Third Session, 32nd Legislature, Ontario.

In *Closing the Gaps*, we urged the temporary creation of a position at the deputy director level to carry out a special official languages plan. In light of developments since then, notably the appointment of the new Deputy Director for personnel and official languages, we have come to the view that this is no longer necessary.

A key personnel issue that we have flagged to the government before is provision for movement between the Service and the Public Service of Canada. Because it would require statutory amendments, it is beyond CSIS's power, and we return to this topic in Chapter 10 below.

As for matters within CSIS's control, it appears to us that the management system is being tightened up in a way that could spare the Service a repetition of some of its past troubles.

5. Counter-terrorism Operations

Counter-terrorism (CT) is one of the two operational branches at CSIS,* and we conducted a thorough study of it in 1987-88. A detailed report is going to the Solicitor General and the Director of CSIS. The report is a long one and its recommendations are classified. This chapter sets out as much as possible of the key findings and conclusions.

CSIS's Mandate

The first issue in other inquiries in this field has been to decide what is meant by "terrorism." One scholarly study cites more than 100 definitions. For CSIS, however, definition is not a problem--its counter-terrorism mandate is set out clearly in paragraph 2(c) of the *CSIS Act*--"activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state".

To combat terrorism, like other threats to the security of Canada spelled out in section 2, CSIS has a mandate under section 12 of the *Act* to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence" and to "report to and advise the Government of Canada".

It is important to note that CSIS does *not* have a mandate to enforce the criminal law, or to collect evidence for criminal prosecutions. This does not seem to be clearly understood by some of the Service's critics. CSIS seeks to identify the sources and targets of terrorism and other threats to the security of Canada. But protecting the targets and apprehending criminals is clearly the responsibility of the police, notably the RCMP under Part IV of the *CSIS Act* (cited as the *Security Offences Act).*

Our Study: Issues and Methods

We began our study with four questions in mind. First, is CSIS doing its part to protect Canadians against terrorism? To answer this question, we looked into the CT Branch's capacity to identify emerging causes of terrorist activity, to analyse their significance, to gather relevant intelligence, and to transmit timely intelligence to those whose responsibility it is to deal with terrorist threats.

The second question was whether CSIS was working within the law, which includes compliance with warrants and with ministerial instructions as well as with the statute itself. It involves matching the Service's policies and procedures with these controls, and matching field practices with the policies and procedures. It also involves questions of accountability-whether each actor, from field investigator to Director, has the responsibilities suited to his or her place in the reporting structure.

We asked, third, whether there was any unreasonable or unnecessary use of the Service's powers in the CT program. A specific concern was whether the Service's interactions with ethnic communities might influence adversely their political, cultural or social activities.

---

* The second is Counter-intelligence (CI). We will study it in the coming year and include our findings and conclusions in our next Annual Report.

Finally, we inquired into whether the *Act* provides an appropriate statutory framework for CSIS's activities in this area. This issue is timely. Any deficiencies in the CT mandate can be cured next year when the Parliament of Canada reviews the *CSIS Act* (the five-year review is discussed in Chapter 10 of this Report).

The SIRC study entailed: examining the structure of CT Branch, and its financial and human resources; interviewing the CSIS officers who implement the CT program across the country; an examination of the many sources of intelligence used by the Service; reviewing operational files; and reading documents, ranging from the papers which identify developing threats to those which analyze past operations.

We studied the use of resources and intrusive powers by target and by region. We did year-to-year comparisons. We examined indicators of the use of covert means of gathering intelligence and asked how appropriately they were being used against different targets.

The Challenge

The first challenge to counter-terrorism investigations is the difficulty of gathering information. Frequently, terrorist groups are organized into cells--closed, coherent units which resist penetration. It is dangerous to get too close to people who use violence to achieve their objectives. Too close for safety is barely close enough for intelligence gathering. It is said that some terrorist organizations will admit new members to the cell only after they have committed acts of criminal violence. The origins of the information used in CT operations is, necessarily, a closely guarded secret.

Another challenge in CT is change. Terrorist personnel, methods and objectives change over time. The terrorist threats under investigation today were largely unheard of in Canada 10 years ago. Will the threats 10 years hence be those of today? The Counter-Terrorism Branch cannot safely assume that they will be. In addition to investigating today's terrorists, an intelligence service must always be looking ahead to emerging dangers.

The events that could bring future terrorist threats can be happening outside Canada. Most--though not all--terrorist threats to the security of Canada are related to conflicts in other lands. And this is a third challenge for CSIS--to maintain an awareness of events in distant places, events that may reflect centuries of human conflict.

The international character of terrorism brings additional challenges of its own. To the extent that terrorist activity in Canada is aimed at targets that represent, actually or symbolically, the interests of foreign countries, these countries take an interest in potential terrorist activity in Canada. CSIS can benefit from exchanges of information with these countries, but it must guard against two pitfalls. The first is providing them with information that will be misused. The other is accepting at face value false information--"disinformation"--that these countries may offer in hopes of making Canada serve their goals rather than its own.

Increased Priority

The emphasis placed on CT has grown dramatically since CSIS was created in 1984. The Air India tragedy was a turning point for the way Canadians think about international terrorism, and for the CT program at CSIS. On June 23, 1985, an Air India jumbo jet on its way from Toronto and Montreal to Bombay went down off the coast of Ireland, taking all 329 people aboard to their deaths. Most of the victims were Canadians. The Canadian government has not officially determined a cause, but public speculation focuses on terrorist violence.

Faced in the same period with government-wide resource cuts, CSIS management initially tried to meet increased demand for intelligence on terrorism within the CT program as it existed. In some offices, overtime reached levels that were inconsistent with both sound personnel management and efficient use of tax dollars. New programs to enhance the cultural sensitivity of field personnel and to process raw information more effectively were deferred.

But existing resources would not stretch indefinitely, and a new tack eventually had to be taken. CSIS shifted its resources around, moving people and materials into priority CT work. More emphasis was devoted to familiarizing intelligence officers with the roots of ethnic terrorism. The procedures for identifying emerging threats and managing long-term threats were improved. Mechanisms for coordinating special events were fine-tuned, and communications with other arms of the government were improved.

These were all improvements. When innocent people are the victims of terrorist attack, the public is entitled to demand the best possible protection. Good intelligence is the first requirement for checking terrorism. So we favour a strong CT program,

Targeting and Investigations

In the study, we examined the targeting policy and procedures laid down in the CSIS Operational Manual, together with all the documents used in making targeting decisions, and we conducted an audit of seven specific targeting decisions. The choice of subjects on our part was largely random. For the warrants which authorize intrusive investigative techniques, such as wiretaps, we checked all outstanding CT warrants, examined some in depth, and reviewed the policy and procedures in the Operational Manual for applications to the Federal Court.

In addition, we made a thorough review of six investigations ranging from long-term monitoring of groups or individuals suspected of making preparations for politically motivated violence, on the one hand, to brief examinations by CSIS of incidents or events with national security implications, on the other.

Targeting and warrant applications are areas where there were dramatic changes in 1987-88 as a result of the "Atwal warrant affair" (see page 14 of this Annual Report). Revisions to the Operational Manual now meet the major concerns we expressed about targeting in our study of the counter-subversion program (Annual Report 1986-87, pages 35-38).

Today, membership in a group suspected of politically motivated violence is not in itself sufficient grounds for targeting an individual in the first instance. Membership in such a group may bring a person to CSIS's attention, of course. But targeting decisions are made on the basis of individual behaviour, and not only group affiliations. We believe this is the proper approach. As we made plain in last year's Annual Report, we do not think people should be targeted solely as a result of being members of groups; targeting should not disregard the nature or extent of their personal involvement.

Although the new policies on targeting and investigation provide all the protections we have advocated in the past, they cause field investigators the opposite concern. Their worry is that, if all their activities must be referable to established threats to the security of Canada, they will be impeded from learning about emerging threats. They should be able to make inquiries--without resort to intrusive investigative techniques--which will permit the Service to discern what their investigative priorities should be in the future. As this Report was being written, the Service was still working out the details of implementing the policies. We urge that a reasonable interpretation be adopted, to permit field investigators to continue the trend towards longer range forecasting of terrorist threats.

We are generally in agreement with the way the CT Branch deploys its resources. With the one exception discussed later in this chapter, the priorities assigned to various terrorist threats are proportionate to the danger they pose. Equally important, Branch priorities take into account impending, as well as immediate, threats. For example, while our study was in course, the Branch, responding to new developments abroad, raised the priority of one form of terrorism that has never produced a violent event in Canada.

The study examined the use, in the CT area, of human sources. The recruitment and handling of human sources is a very delicate business. In addition to the common frailties of human nature, CSIS investigators must concern themselves with motive and reliability.

We found that CT practice as well as policy is to be very careful that sources are directed only against properly designated targets and collect only the kind of information that is properly CSIS's concern under the *Act*. We found CSIS policy on the recruitment of human sources, on source development and on verifying expenditures to be satisfactory, and we found no breaches of that policy.

Our examination of physical surveillance included discussions with officials involved in carrying out this work, a review of the Operational Manual, an examination of internal audits of the program, and a review of all reports about surveillance against CT targets in two regions for a one-month period. We came away very impressed with the competence and resourcefulness of the surveillance operation.

The study looked at the use of technical intercepts, including the processing of intelligence from technical sources. Last December, during the investigation of the Air India tragedy. it was revealed that the Service had erased audio tapes. CSIS operates under a policy which provides for retaining evidence of crime. There is also provision for notifying the police when life-threatening situations are discovered. In general, however, the policy is to transcribe relevant information from intercepts, and then erase the tapes. This prevents

the retention of information about people's private conversation as that information is not relevant to the security of Canada. At the time of writing, we have still not reached any final conclusions regarding tape erasures in the Air India case.

Policies and Practices

Collecting information is what CSIS does best. Our research convinced us that the general quality of the intelligence gathered by the CT Branch is very good. The Branch has a creditable record in tracking the movements and activities of its targets.

It also shows a healthy skepticism about information from foreign intelligence agencies. There are, inevitably, some wild goose chases as a result of inaccurate or misleading information from other agencies; CT is an area where mistakes can cost lives, so no information can be ignored. But the Branch takes into account the foreign policies of countries that supply information and may try to twist Canadian CT activities to their own purposes. It also takes into account the track record of foreign agencies in supplying information that has proved valid--or not--in the past.

In its ongoing investigations, the CT Branch does not intrude unduly in the affairs of ethnic communities. Its attention is focused on clearly established threats to national security, not on entire ethnic groups. We came across one case in which CSIS was repeatedly asked by members of one ethnic community for advice on counter-measures that the moderate majority could use to prevent a minority from manipulating community events for political ends. CSIS's response was restrained and appropriate.

There is a problem with the Canadian chapters of foreign groups which engage in terrorist acts to overthrow the governments of their homelands. Under the *CSIS Act*, the Service is to gather information "to the extent that it is strictly necessary". While the Canadian supporters endorse the objective of the foreign terrorists, their activities here, in many cases, consist largely of political advocacy and protest. Not all conflicts abroad spill over into terrorist attacks internationally.

Where there is no apparent risk of violence within Canada, the Service must take special care to ensure that it is not investigating "lawful advocacy, protest or dissent" except where it is carried on in connection with terrorist threats. It must also be sure to recognize situations where threats are diminishing; that is, as violent conflicts peter out abroad, investigations of Canadian support groups must be scaled back or proportionally reduced. This is particularly necessary in areas such as Latin American conflicts, where the political currents in the homeland are constantly shifting. Our study identified one situation in Latin America where, we concluded, the Service had been slow to shift its attention away from such a group as the group's contribution to the conflict abroad dwindled. Although the targeting of the members of the group is lawful under the *Act*, we felt the scope of the investigation was exaggerated.

We also have some concern about the possible by-products of Service activities in connection with special events like the Commonwealth Heads of Government Meeting. In

advance of such events, the CT Branch interviews mainstream members of ethnic communities that have terrorist elements on their fringes. Its purpose is to gather information about potential threats.

But there is another, incidental effect: these interviews remind everyone in the community that CSIS is watching and, thus, warn off extremists. It is all to the good if terrorists are deterred. But we fear that the inhibiting effect could extend throughout the community concerned if the practice is not controlled. Feeling that they are under the eye of the, authorities, other members of these communities could be discouraged from exercising their rights of legitimate and lawful dissent. This is a continuing dilemma for the Service requiring careful and continued attention each time there is a "special event".

Intelligence Production

Under section 12 of the *CSIS Act,* the Service's core role is to provide intelligence and advice to the government. We checked with a number of federal agencies that are the principal consumers of CT intelligence and found that they are generally satisfied with the quality of the intelligence they get on terrorist threats. They are also generally satisfied with their access to CT personnel to discuss issues and problems. Information given to consumers on how to identify suspected terrorists is well received. So are analyses which describe the level of danger to particular interests from particular terrorist organizations.

A continuing problem is the different approaches of CSIS and the police to terrorism. CSIS believes that, in certain cases, the police would like the Service to use its investigative powers in support of the police role, which is law enforcement. But this is not what CSIS was created to do. It was created primarily to provide advice on the basis of its analysis of information from both open and covert sources. Of course it has a duty to assist the police when and where it can. But its emphasis belongs on gathering information over gathering evidence in a form that can be used in court. CSIS has done its job when it has pinpointed a threat and told police about it. It should not then endanger the effectiveness of its procedures in order to accumulate evidence that can be used in laying charges and securing convictions.

Co-operation between CSIS and the RCMP has improved considerably. This is due in no small part to the exchange of Liaison Officers between the two agencies. The differences in emphasis between intelligence and evidence inevitably continues to cause some strain. CSIS insistence on protecting its sources sometimes leaves the police wondering whether they are getting all the information they would like.

In our own examination, we found that the CT Branch is at its best in dealing with current threats. It is an operational branch and most of its intelligence products serve immediate operational purposes. The Branch also produces assessments of long-term trends in countries from which there is no immediate threat to Canada. While this is probably the least important product of the Branch, these assessments are not up to the standards of the intelligence produced by the Analysis and Production Branch, discussed in the next chapter.

The same unit which carries out research within the CT branch also prepares briefings for senior officials, notably the Director of CSIS. The briefing function, with its more immediate deadlines, tends to displace the intelligence function. We think it is good that the Director meets personally with other parts of the intelligence community and naturally he must be well-briefed for such meetings. But we do not think that briefings and operational research co-exist well in the

Research and Briefing Unit. Each has an important role in the CT Branch. We would like to see these roles expanded--and separated.

If the Director gets around, operational analysts in the CT Branch do not. They are given few opportunities to attend national or international meetings on terrorism. We think they should be given more opportunities to meet with their counterparts and colleagues in other countries so each understands the other's work better and, when events are developing quickly, there are personal as well as working relationships to help oil the machine.

Conclusion

At the end of our study, we were broadly satisfied with the answers we found to the four questions we started with. We found that the CT Branch provides adequate protection to Canadians. It stays within the law. The *CSIS Act* provides a suitable framework, dividing CSIS's intelligence role from the law enforcement role of the police.

In the Counter-Terrorism Branch, CSIS is showing that it can gather information in a forward-looking manner which goes beyond supporting law enforcement activity.

In areas where the Branch has historically been weak, such as analysis, we discerned pronounced improvement. The areas where the need for further improvement is greatest are in long-term strategic analysis, which we discuss in the next chapter of this Annual Report.

6. From Information to Intelligence

Information is the raw material that CSIS works with. The finished product is intelligence--information sifted and arranged in such a way as to help users make the right decisions. CSIS has an Analysis and Production Branch (APB)* whose job, in the words of the Operational Manual, is "to produce intelligence assessments in concert with the operational branches and facilitate the flow of information to the relevant decision makers in the Government of Canada".

APB produces papers called *CSIS Reports*, each summarizing current intelligence on a single topic, organization or person, and special reports that go into more depth. It also contributes papers and information to the Intelligence Advisory Committee (IAC) and the Security Advisory Committee (SAC). These are the key subcommittees of the deputy minister-level Interdepartmental Committee on Security and Intelligence (ICSI) which reports, in turn, to the Cabinet Committee on Security and Intelligence, headed by the Prime Minister. Overall, APB output exceeds 250 documents a year.

We conducted a review of the intelligence analysis and production process in APB in 1987-88. But CSIS is not alone in this field; the Departments of External Affairs and National Defence, to take the most obvious examples, have significant capabilities of their own, and many arms of the federal government make use of security intelligence. So our inquiries inevitably led us to consider CSIS's relationships with other agencies, both producers and users.

In carrying out the review, we met with APB staff at all levels--the Director General of the Branch, present and former section chiefs and a number of working analysts. We followed some draft *CSIS Reports* through the process, looked at work done for IAC and sat in on the deliberations of the APB Intelligence Production Committee. We also had discussions with other agencies that use CSIS intelligence, studied the training, experience and academic qualifications of APB analysts and reviewed the relevant scholarly literature. We drew on a user survey carried out by the Branch itself in 1987-88.

A full report is going to the Solicitor General for his consideration. This chapter reviews key findings and issues.**

The Intelligence Product

We adopted the distinction made by the Solicitor General's Independent Advisory Team between operational and strategic intelligence.*** *Operational intelligence* is "related to the investigation of particular activities considered threatening to the security of Canada". It "relies heavily (but not exclusively) on investigative techniques, is usually short-term and is produced for specific consumers or for a specific purpose". This is "case-oriented" intelligence, and CSIS itself is a major consumer as well as a major producer. Operational intelligence is the province of the operational branches of CSIS, Counter-terrorism and Counter-intelligence, and they have their own staff analysts.

---

* Formerly called the Intelligence Assessments Branch (IAB).

** APB also keeps a watching brief on low-level counter-subversion targets (see Chapter 3 above), but our study focuses on the assessment and production process as such.

*** *People and Process in Transition*, pages 18 and 39.

APB produces *strategic intelligence*. This intelligence "relies more heavily on research using information from all sources, tends to be longer term and more global in scope and is produced for an interdepartmental audience or for the government as an entity". It "is evaluated in the context of other Canadian national interests". Within the strategic category, we distinguish current from basic intelligence. *Current intelligence* focuses on events as they unfold and alerts decision-makers to potential emergencies. *Basic intelligence* is in-depth data on countries and subjects, which should help the government in the development of policy and in strategic decision-making.

To illustrate with the example of a meeting between two individuals suspected of being threats to the security of Canada, operational intelligence would determine that the meeting took place and report, if possible, what was said. Current intelligence would put the meeting in context--identifying what organization these people belong to, for example, and suggesting what this meeting may reveal about possible changes within the organization and its plans. Basic intelligence provides the larger context by assessing the capabilities, intentions and vulnerabilities of the organization.

Current intelligence accounts for most of APB's production. This is reflected in comments by users that what *CSIS Reports* do is alert them to specific issues--weapons sales, for example. We see a gap; the government is not getting all the basic intelligence it needs. A steady stream of current intelligence reports can result in security intelligence being dealt with as a series of "flaps" rather than as an ongoing, long-term process.

Setting Priorities

The reasons for APB's emphasis on current intelligence can be found partly within CSIS itself. But the ultimate responsibility for determining intelligence requirements and setting priorities lies not with CSIS but with the government. It is a common criticism in the security intelligence field throughout the Western world that governments do not give their intelligence agencies clear enough direction, and this appears to be true in Canada.

In the absence of clearer direction from the government, a number of factors within CSIS have encouraged the emphasis on current intelligence. One stated by CSIS officials we spoke to is the inexperience of much of the APB staff. About half the Branch's analysts are newcomers to security intelligence since CSIS was created in 1984, and they are cutting their teeth on short-term, current intelligence projects. More experienced analysts are deflected from basic intelligence production by the need to spend time guiding their juniors. This, we were told, will change as experience grows.

Perhaps so, but there are also entrenched institutional factors. For one thing, APB does not have a unit devoted solely to producing basic intelligence. More far-reaching is the influence of the operational branches over APB.

A major role in setting APB's program is played by the operational branches through the Intelligence Production Committee (IPC) within CSIS. IPC is headed by the director general of APB, but the directors general of the operational branches have most of the votes. There is a higher level "executive" IPC of deputy directors which ought to be providing a broader perspective, but it is largely inactive. It met only once in 1987. The director-general-level IPC

(which is what we mean by "IPC" in the remainder of this chapter) has naturally filled the vacuum.

After determining where APB analysts will focus their attentions, IPC comes into the picture again at the end of the production process when it comments on the final draft of each report, may order revisions, and decides on distribution to client departments and agencies, to CSIS security liaison officers abroad and to friendly foreign security and intelligence agencies.

Sources and Methods

Analysis relies on a number of sources--information gathered in investigations by operational branches, the security liaison officers, open information such as the mass media and publications by experts, the security and intelligence agencies of friendly countries, and other parts of the Canadian intelligence community.

The influence of the operational branches continues after a topic for analysis has cleared IPC. The APB analyst often works closely with a counterpart in the relevant operational branch. Much of the raw information used by the APB analysts is from operational sources. The operational officers often check the APB conclusions. The resulting paper sometimes goes to the director general of the operational branch for review before it reaches the APB analyst's own chief and the APB's own Review Committee.

A more subtle influence, at least for the immediate past and the immediate future, is that many of the APB analysts have less experience and less status than their operational counterparts. In addition, most APB analysts are attached to operational branches. They even have their offices in the quarters of the operational branches they work with instead of being all together, so the corporate culture they absorb from their surroundings is operational rather than analytical. In one section, the Chief’s office is in a different building from the offices of most of the analysts under him.

We were glad to find that APB's reliance on open sources is growing. Readers of our annual reports will recognize maximum reliance on open information as one of our signature themes (see, e.g., page 17 of this Report). Our inspection of user data for 1986-87 and 1987-88 showed a 10-per-cent increase in APB requests for open data from the CSIS Information Centre.

We have also had occasion in the past (Annual Report 1986-87, page 23) to remark that CSIS might be too ready to accept information supplied by friendly agencies in other countries at face value. We were told in our APB review that analysts cast a critical eye on information from allies with axes to grind on specific issues. In addition, corroboration from other sources was a criterion in assessing information from other agencies; in theory, such information should not be accepted before it is confirmed elsewhere.

But confirmation is not always easy, and APB section chiefs do not have enough access to computer terminals that would let them double-check source documents. Incidentally, this and other inadequaciesin physical arrangements are small but telling signs of inadequate day-to-day attention at the top to the Branch's work. In our discussions with intelligence users, the point was sometimes raised that *CSIS Reports* did not always pay sufficient attention to Canadian implications. Other users, however, stated that APB efforts to put more emphasis on "Canadian considerations" are apparent.

As to analytical procedures, no models have been set by APB for its analysts to follow. IAC and SAC expect work done for them to be in a specified format. But, generally speaking, APB counts on each analyst to select a framework suitable to the matter in hand. We do not suggest methodological strait-jackets in which the facts are selected to fit the format instead of the format being shaped by the facts, but we are concerned that the absence of ground rules makes it difficult to assess analysts' work. A middle way needs to be found.

New APB analysts follow a special course at the Service's Sir William Stephenson Academy, but it focuses on operational analysis. It does not encompass political and strategic analysis. This is a gap that must be filled quickly. There is a consensus among APB managers that more specialized intelligence assessment training should be available, and we hope that discussions now underway will soon bear fruit.

Specialization

We also have some concern about obstacles to the development of world-class expertise within APB over the years. The prevailing view within CSIS is that analysts should be generalists, not specialists. We see advantages in this approach. It lets the analysis function adjust more quickly to changing priorities. It encourages fresh thinking as a wide range of knowledge and experience are brought to bear on topics.

But these advantages are vastly outweighed in our view by the need for in-depth knowledge. Generalists are less likely, for example, to be attuned to the cultures of the group they are studying. They will be ill-protected from thinking in stereotypes and less able to pick out significant nuances.

The bias to generalization is more than a matter of attitudes within CSIS. It has strong organizational underpinnings that will perpetuate it indefinitely unless there is a clear and specific decision to encourage specialization.

Analysts rank in the "journeyman" IO-1 to IO-3 levels in the job classification scheme. Once they have reached the IO-3 level they may have difficulty moving into entry-level positions in the operational branches. Yet they can advance no further within APB unless they become managers rather than analysts. This eliminates the hope of higher pay and higher status as a reason to do the independent study that specialization requires under present circumstances. In addition, the present classification levels are not likely to attract specialists from other branches or from outside the Service.

We think that there should be senior--specialized--analysts classified above the IO-3 level. In this connection, we think APB could be a good place to locate suitable CSIS liaison officers when they come home from assignment abroad. Intelligence production could benefit greatly from their extensive experience. But they hold ranks well above IO-3, so APB is not now an attractive destination for them.

Two other institutional constraints on specialization are discussed in a broader context in Chapter 10, so we will simply mention them here. Members of CSIS are encouraged to remain publicly anonymous, so they seldom present papers at conferences. Indeed, the Branch does not have sufficient resources even to send analysts to conferences. (CSIS does, however, have an in-

house program of seminars and presentations involving people from other parts of the security intelligence community, Canadian and foreign). Second, there are statutory obstacles to transfers and secondments between CSIS and the Public Service.

Meeting User Needs

It is a welcome sign of Branch management's commitment to improving its product that it conducted an extensive survey of users in 1987-88. We found it a useful supplement to our own interviews with users. We are not as impressed with the user questionnaire circulated with each *CSIS Report* which invites superficial responses. We are also concerned that the Branch does not systematically evaluate its own work in light of subsequent events, and we urge that it start doing so.

Nonetheless, and despite some criticisms, the consensus within the security intelligence community is that the assessments provided by APB are getting better. We found that there was still too much description and not enough analysis, but APB's efforts to right the balance and to focus more on the "Canadian implications" section of its reports are also evident. APB acknowledges the justice of complaints that its conclusions need to be better substantiated.

Timeliness was one problem flagged by users; they said they were not getting *CSIS Reports* quickly enough. Urgent briefs and reports are distributed electronically for the sake of speed, but a degree of slowness is built into the system. Part of the blame must go to a cumbersome approval process for APB papers. As more analysts gain more experience, it should be possible to bypass the Review Committee composed of APB chiefs; each chief could take responsibility for the work of the section and send it directly to the IPC. At the least, the Review Committee needs to be given formal terms of reference.

Translation delays are another problem. A 1- to 3-page document takes no less than a week to translate. Documents of more than 20 pages require four weeks or more. APB could speed the process itself by following the common practice of sending an early draft to translation, so there are only revisions to be made when the document is in final form. However, as we have in other contexts, we also urge CSIS to make sure it has enough translators to meet the demands of government-wide official languages policy.

Some users said that the classification of *CSIS Reports* as SECRET limits their usefulness, since they could not be given without censorship or special dispensation to some people who could benefit from them but did not have the required security clearance. Liaison was also identified as a problem by some users; APB recognizes the need to brief users directly on some issues of special concern to them, to ensure that the implications of the intelligence provided are drawn out and that user needs are well understood.

Options for the Future

Among our key findings were an emphasis on current rather than basic intelligence and, in the absence of clearer direction from the government, the great influence of the operational branches on APB. These two matters are related. The operational branches raise issues for analysis, influence its production through the information they provide and through formal reviews, and ultimately decide what will be circulated.

CSIS management needs to consider whether it wants to maintain the status quo, producing mainly current intelligence under strong operational influence, or give APB the resources and organization it needs to develop more basic intelligence. In either case, we believe that IPC should have proportionately fewer members from the operational branches and more from APB itself. Drawing on its perspective as a service to the government as a whole, APB needs to have more influence over its own analysis priorities and over the content of the intelligence that it disseminates.

Another option for consideration by the Government would be the creation of a separate assessment agency on the Australian model to produce basic intelligence. Such an agency would not replace APB, which would continue to produce current intelligence. The overlap with present Canadian structures would be more with IAC, though it acts as a clearing house and coordinator rather than as an intelligence producer.

When we visited Australia, we paid particular attention to the role of the independent Office of National Assessments (ONA) there. The Australian Security Intelligence Organization (ASIO), which corresponds with CSIS in Canada, collects and distributes information and analyses intelligence principally from an operational point of view. ONA is an assessor, not a collector, and it is an external agency, not an internal one. That is, it does not collect intelligence but uses intelligence and other information, including from open sources, to produce reports, appreciations and assessments, and it is directed not to the internal security of Australia but to international, political, strategic and economic matters of relevance to Australia.

Australian officials are convinced of the value of independent intelligence assessment. Away from, though not unaware of, the urgent demands of day-to-day operations, ONA can concentrate on long-term requirements. There is little temptation to expend resources on "data-driven" work -- that is, analysing whatever happens to have been turned up through investigations by the collecting agencies. Studies are "need-driven". They must be directed to a clear objective and have at least the potential for leading to recommendations for specific government action. In fact, as a full member of the Secretary's Committee that serves the cabinet and also through its assessment of where problems are likely to arise or where available information is too sparse, ONA plays an important role in setting priorities for the collecting agencies, including the Department of Foreign Affairs and Trade, whose normal diplomatic reporting is a prime source of ONA's information. ONA is the institutional critic of the quality and quantity of information the collecting agencies provide.

ONA's access to expertise also impressed us. Most ONA analysts have post-graduate degrees and they rarely remain on staff more than five years, so there is a constant infusion of the latest knowledge and thinking from the worlds of scholarship and the professions.

We want to make it clear that we are not at this point recommending imitation of the Australian model. We have not had an opportunity to examine this matter thoroughly enough for that. We also recognize significant differences between APB's role in CSIS and ONA's role in Australia. But we believe a separate agency is an option the Government might consider if it shares our view that it needs more basic intelligence.

Summing Up

Before CSIS was created in 1984, the history of assessment units in Canadian security intelligence was a record of failed starts. That has changed. We found that APB is moving more and more towards producing the kind of intelligence that SIRC believes the government needs.

Branch managers have taken important initiatives to ensure that their product becomes as good as it can be under present circumstances. We have mentioned the user survey, which was carried out well. Memoranda of understanding have been signed with the operational branches, to ensure that the division of responsibilities is well defined. APB has won the respect of the operational branches and, with it, the access it needs to sensitive information held by these branches.

However, APB can only go so far on its own. In particular, Service-wide personnel policies are an obstacle to hiring and developing specialists with an intimate understanding of the social and cultural backgrounds of CSIS targets. Service management's undoubted cornmitment in principle to analysis and production does not seem to be followed through day to day.

We believe that Canada will only get the best strategic intelligence possible when APB enhances its corps of professionals in order to produce policy-relevant analyses. They should draw on the whole range of information available to the government and rely less on the product of field investigations. If such a group does not fit within CSIS, the Government could consider creating one elsewhere.

7. Complaints

As we have already explained, we have a dual mandate under the *CSIS* Act--oversight and complaints. Paragraph 38(c) of the *Act* directs us to investigate complaints that anyone may make about the activities of the Service and complaints about the denial of security clearances in Public Service employment, in the supply of goods and services to the Government of Canada and in immigration and citizenship matters. We also investigate the security aspects of certain complaints lodged with the Canadian Human Rights Commission.

Summary case histories of investigations completed in 1987-88 can be found in Appendix B of this Report. In this chapter, we provide an overview and discuss current issues in the complaints process.

The 1987-88 Cases

We took in 38 new complaints in 1987-88--exactly twice as many as the year before (see Table 3 below). Complaints about the denial of security clearances and about security considerations in immigration remained at 1986-87 levels, one and two respectively. Complaints about an intention to den citizenship for reasons of national security or involvement in organized crime fell to one in 1987-88 from two the year before.

But the number of complaints under section 41 of the *Act* rose by a factor of 2.6. Section 41 provides that "any person" may lodge a complaint "with respect to any act or thing done by the Service". We must investigate if three conditions are met--first that the Director of CSIS has already had a chance to deal with the matter, second that we are satisfied the complaint is not "trivial, frivolous, vexatious or made in bad faith" and, finally, that there is no other avenue of redress under either the *CSIS Act* or the *Public Service Staff Relations Act*. These complaints numbered 34 in 1987-88, compared with 13 the year before.* We also carried two such cases over from 1986-87.

There was no pattern in the nature of the section 41 complaints. The increase simply seems to reflect growing public awareness of our Committee and its work rather than any particular failing on CSIS's part. Thirty complaints could be dealt with quickly; either they were clearly out of our jurisdiction or the complainant offered no factual base on which an investigation could proceed. We completed the investigations of two complaints. In neither did we find any wrongdoing by CSIS.

In one security clearance complaint, we recommended that the clearance be granted. It is too early to know whether our recommendation will be accepted. Among the citizenship cases, three files were closed before we completed our investigation, because CSIS withdrew its objections. We agreed in the fourth case that citizenship should be withheld. In immigration, we agreed with deportation of one individual and in a second case, which involved criminality, the file was closed before investigation was completed because the RCMP withdrew its objection to the individual's entry into Canada.

---

* In this discussion, we do not take into account more than 2,000 complaints made by CSIS employees in 1985-86 and 1986-87 about the official languages practices of the Service. These complaints have been dealt with through a special inquiry, which we published in 1986-87 under the title *Closing the Gaps*.

As can be seen in Table 3, we closed 39 complaint files in 1987-88. With 14 files carried over from the previous year and 38 new complaints, this left us at year-end with 13 files open. This is a manageable number--one less than we had at the same time a year earlier.

Table 3. The Complaints Record, 1987-88

	New complaints	Carried over from 1986-87	Closed	Carried over to 1988-89
Security clearances	1	1	1	1
Citizenship	1	7	4	4
Immigration	2	4	2	4
Section 41	34	2	32	4
Total	38	14	39	13

Who Decides?

An issue of great long-term significance came to a boil in 1987-88 when the Federal Court of Appeal stated as *obiter dicta* in *Thomson v. The Queen* that deputy ministers are bound by our recommendations on security clearances in Public Service employment; when we conclude after investigation that a clearance has been unreasonably withheld, the deputy minister concerned must act on our recommendation to grant that clearance.* Continued refusal could, the Court said, be justified by new information that came to light after our investigation was completed. But such a refusal could, of course, give rise to a new complaint for our adjudication.

However, no one expected that this would put an end to the question. Nor did it. For jurisdictional reasons, the same matter came before the Trial Division of the Federal Court for decision soon afterwards, and the ruling went the other way; deputy ministers are not bound by our recommendations, said Mr. Justice Dubé of the Trial Division.** Now this decision is under appeal.

The matter arose in this way. Robert Thomson was the successful candidate in a competition for a position in the Department of Agriculture. The position required a security clearance at the SECRET level (now called Level II), so his appointment was conditional upon his receiving this clearance. After making inquiries at the request of the Department, CSIS recommended against clearance. A number of allegations against Mr. Thomson are on the

---

* Unreported decision of the Federal Court of Appeal, March 7, 1988.

** Unreported decision of the Federal Court of Canada Trial Division, June 15, 1988. This decision came down after the end of the year covered by this report, but we feel it is necessary to take note of it here; to do otherwise would give a very misleading picture of the situation.

record, including the fact he "leaked" at least one document that came his way when he worked for the Canadian International Development Agency some years ago. After consulting both his own officials and the Privy Council Office, the Deputy Minister denied the clearance and the offer of employment was withdrawn.

Mr. Thomson thereupon complained to us. In accordance with our normal procedures, two of us conducted an investigation. Mr. Thomson, the Department and CSIS were all represented by counsel. The conclusion was that Mr. Thomson "would be unlikely to release classified information if he were once again employed in a position with access to such material". We recommended that Mr. Thomson be granted the SECRET clearance so he could take up the position. The Deputy Minister stood by his original decision, and Mr. Thomson applied for relief to the Federal Court of Appeal.

That was when the Court of Appeal said that the Deputy Minister did not have a choice in the matter: he was bound to follow our recommendation. But the Court did not have jurisdiction to set aside the Deputy Minister's decision, as such orders are the prerogative of the Trial Division. Mr. Thomson accordingly turned to the Trial Division, bringing Mr. Justice Dubé's ruling.

Until the Courts have ultimately disposed of this case it would be inappropriate for us to comment further on the merits of the legal issues involved.

Disclosure

We have an on-going tug-of-war with CSIS over the disclosure of information to complainants. Recognizing the Service's responsibility for guarding national security, we are always reluctant to give complainants information against its advice. But we have a responsibility to ensure that complainants know enough to make an informed response to allegations that have been made against them.

Section 46 of the *CSIS Act* sets out this duty with respect to the denial of security clearance in government employment and government contracts. It says we must give the complainant "a statement summarizing such information available to the Committee as will enable the complainant to be as fully informed as possible of the circumstances giving rise to the denial of a security clearance". In principle, the complainant should have all the relevant information available to us, subject to the "as possible" limit. The principal constraint we accept in providing information to complainants is that CSIS sources must be protected from exposure. There are similar provisions with respect to citizenship and immigration complaints.

In both Australia and New Zealand we were told that disclosure is not a problem. The president of Australia's Security Appeals Tribunal said that the Australian Security Intelligence Organization, which corresponds to CSIS in Canada, is generally cooperative about providing complainants with enough information to permit a full defence. In New Zealand, Sir Thaddeus Pearcey McCarthy, the Commissioner of Security Appeals, told us that he always gives complainants all the details of the allegations consistent with concealing sources.

Here in Canada, we have found that CSIS is overly cautious in its view of how much complainants can be told, and we have often had to take a strong stand. CSIS still finds this process disorienting. In one case, CSIS withdrew its objections to citizenship for an individual rather than have us reveal information that we thought the person needed to mount a reasonable defence.

8. Inside SIRC

Our operational activities in oversight and complaints have been described in the foregoing chapters. Still to come are chapters on two broad issues that transcend the daily grind--our work to foster informed public discussion of security and intelligence issues and, second, some matters that Parliament and Canadians may want to consider when the *CSIS Act* is reviewed in 1989. In this chapter we put some housekeeping details on the record.

Our Work as Members of SIRC

Much of the day-to-day work of our Committee and much of the research is conducted, of course, by our staff. But we are all personally active in the oversight and complaints process. We meet as a Committee at least monthly to discuss issues and make key decisions. We work individually with staff on such projects as the counter-terrorism study reported in Chapter 5. Hearings on complaints are conducted by us in person, but with hearing panels usually of one or two Members established by the Chairman to spread the work around.

We continue to believe that there is value in having a part-time, all-party Committee like ours to provide oversight and investigate complaints. The tri-partisan nature of the process by which we are appointed under the *Act* is an assurance to Parliament and the public of impartiality. Yet it has not been an impediment to the collegial approach we have taken to our work. The fact we are not permanent officials is also valuable. Being active members of our communities in different parts of the country probably helps maintain the degree of detachment appropriate to an oversight body.

Financial Report

Our 1987-88 spending is set out in Table 4.

Table 4. SIRC Budget 1987-88

Personnel		$565,000
Salaries and wages	$491,000	
Contributions to employee benefit plans	$74,000	
Goods and services		$661,000
Professional and special services	$507,000	
Other	$154,000	
Total operating expenditures		$1,226,000
Capital expenditures		$9,000
TOTAL		$1,235,000

Source: 1988-89 Estimates, Part III

Personnel

Our staff still stands at 13, headed by an executive secretary who directs all day-to-day operations. Other employees are a research director, two research officers and a research assistant, a senior complaints officer, an executive assistant who supports our research and complaints functions, an administration officer who doubles as registrar for our hearings and triples as coordinator of our responsibilities under the *Access to Information Act* and the *Privacy Act*, a records officer, a records clerk and three secretaries.

9. Need to Know

One of the most-used phrases in security and intelligence is *need to know*. In CSIS and its counterparts worldwide, information is relayed on a need-to-know basis. Each fact, each idea is imparted only to those who need it to carry out their work. Everyone else is kept in the dark. Thus the risk of leaks is lessened--and the circle of suspects is limited if a leak does take place.

There is another need to know--the public's need to know what is being done in its name. Many details of security and intelligence work must, of course, remain secret for the obvious reason: publicity would arm democracy's foes. But much can be told without danger to national security, and it should be told.

Intelligence Directory

We mentioned last year that, when SIRC was created, we found many of our questions were not readily answered from available materials. For example, as newcomers to the world of intelligence, we wished for a comprehensive directory of federal agencies engaged in security and intelligence.

All the agencies helped us to compile that directory ourselves. It has proved useful for other newcomers, including CSIS recruits.

We have now produced an expurgated version for public consumption and are publishing it as Appendix C of this Report. We caution that it is purely descriptive; nothing in it is to be taken as an assessment of the various organizations it describes.

Reaching Out

The directory is one example of a conscious effort to increase public understanding of security intelligence issues and to make CSIS's work better known. The annual report is our major vehicle. We prepare it primarily to meet a statutory obligation, of course, but we are also conscious of the contribution it can make to informing Parliament, academic and other specialists, the media and (largely through the media) the Canadian people. In the absence of any other open source, it provides the only statistics available to Canadians generally on warrants granted to CSIS. It has let us keep debate going on issues like the use of open sources and targeting procedures.

The annual report forms the basis for appearances before Parliamentary Committees. During the year under review, we appeared before the Standing Committee of the House of Commons on Justice and Solicitor General on December 17, 1987 (with a second appearance shortly after the turn of the fiscal year, on April 14, 1988).

As explained in Chapter 2 above, we also make special reports to the Solicitor General, and some of these are made public. Our special report on *CSIS' Use of its Investigative Powers with Respect to the Labour Movement* was released in March, 1988 (see Chapter 3 above for a review of key findings). Last year, we published *Closing the Gaps*, an abridgment of our report to the Solicitor General on official languages practices and staff relations in the Service.

Another important vehicle for public information is our speaking engagements before interested publics. The Chairman, Ronald G. Atkey, delivered a paper on "Accountability for Security Intelligence Activity in Canada" on May 8, 1987, at the Osgoode Hall Law School conference on Domestic Security: Issues for Democracy. Jean Jacques Blais spoke with political science students at Carleton University in Ottawa last fall, while Paule Gauthier touched on the work of our Committee in an address to the Association of Federal Women Lawyers in January, 1988, and addressed the Political Science Department at Laval University in Quebec this spring. As the year ended, Mr. Blais was preparing an address on "the Political Accountability of Intelligence Agencies--Canada" to the 1988 conference of the Canadian Association for Security and Intelligence Studies.

We are frequently in touch with the media, which look to us for information and background when security intelligence stories erupt. We held a news conference when our last Annual Report was tabled in June, 1987.

Canadian Scholarship

We have also acted on the need we see for Canadian scholarship in security intelligence issues. So much of our knowledge and thinking about these matters in Canada has been based on the study of American and European experience.

Back in 1985, wanting to prepare ourselves for our responsibilities in launching SIRC, we sponsored a seminar where about two dozen scholars in relevant disciplines and other experts shared their knowledge and their perspectives with us. Some of the issues we discussed back then are still at the heart of our approach--our concern for striking a balance between the protection of fundamental freedoms and effective intelligence gathering, for example.

This year we participated in the sponsorship of two conferences. The Centre for Public Law and Public Policy at Osgoode Hall Law School put on a conference at York University May 8-9, 1987, on Domestic Security: Issues for Democracy, which we underwrote. Then we shared sponsorship, with the Office of the Inspector General, in a conference on Advocacy, Protest and Dissent at Queen's University in Kingston February 25-27, 1988. There is no need to review the proceedings of these conferences here as they are to be published--except to say that they made an important contribution to the goal of informed debate.

Members of our staff sometimes make individual contributions. One of our researchers presented a draft paper at an international colloquium staged at the University of Seville in Spain February 25-27, 1988.*

He quarrels with the view that without media attention, terrorism would wither away. When, for example, authorities buckle under pressure to save innocent lives, sometimes in

---

* M. Klein, *Terrorism and the Media: A Social Learning Approach*, a draft paper presented to the Ninth International Colloquium on the Brain and Aggression, University of Seville, February 25-27, 1988. Views expressed in this paper are the author's, not necessarily the Committee's, but we agree with the views cited in this Report.

the face of negative international publicity, terrorists are confirmed in their view that violence gets results. Bonding within the terrorist cell and the "heroic" standing that the individual terrorist enjoys among sympathizers also give terrorism a life of its own.

But modifying the behaviour of the immediate targets through aggression and violence is seldom the whole terrorist agenda. By courting media coverage, terrorists seek to spread their propaganda, to demoralize the public and the authorities, for example, or to appeal to new sympathizers and awaken potential recruits.

Media: Friend, Foe ... or Both?

Clearly the media play a key role in the contemporary rise and spread of terrorism and in the way individual acts of terrorism unfold. In general, the mass media are a positive force in fostering informed discussion of security and intelligence matters. There is no other institution in society with their reach and their ability to present issues in terms that most people can understand. But we are not blind to the problems that can arise in reporting on terrorism and on security intelligence generally. In the opening chapter of this Report, we commented on the atmosphere of suspicion that swept the Canadian media in the wake of some real CSIS problems, leading to some questionable reporting. And when terrorists earn points simply by making news, then reporting news about terrorists is a minefield.

Specific instances in Canada of conflict between the public's right to know--which is served by the media--and legitimate security requirements have been documented by the Senate Committee on Terrorism and Public Safety.* Instances abroad are well known--the "Beirut Syndrome", for example, in which major media go along with terrorist conditions on the dissemination of information.

It is not realistic to expect the media to stop reporting on terrorism. It is not desirable, for the public needs to know how the game of politics is being played, whether by fair means or foul. But we readily endorse the observation in *Terrorism and the Media: A Social Learning Approach* that "it is important that reporters be sophisticated enough to realize when and how they are being manipulated by terrorist movements". Sometimes the issue is simply one of timing: does the public need a breathless live report the minute the SWAT team moves into position or can it wait a few hours? Sometimes the issue is more complex: should reporters accept the role--as some Irish reporters have--of uncritical conduit for terrorist propaganda for the sake of the nuggets of exclusive information that come their way as a result?

Speaking Up for CSIS

Another aspect of the public's need to know is its need for a realistic picture of CSIS. We accept some responsibility. Our Executive Assistant stressed realism when she spoke to the Centre for Investigative Journalism at its 10th annual conference in Toronto, March 25-26, 1988. James Bond is fun but fiction, she said. "The truth would be better served if the cloak-

---

* Senate of Canada, *Report of the Special Committee of the Senate on Terrorism and Public Safety* (Ottawa, Supply and Services Canada, 1987).

and-dagger symbol for espionage were changed to that of a typewriter and some 3x5 index cards."

CSIS itself has a responsibility, of course. We have previously urged (Annual Report 198687, page 46) that it undertake a public relations campaign designed to foster an appreciation among Canadians of its role. We saw this primarily in staff relations terms, as a means of creating a positive corporate image to back up a shared sense of personal contribution to the security of Canada among all employees. But it would serve the goal of public information as well.

We particularly welcome the recent efforts of the Solicitor General to increase public awareness and understanding of the valuable work that CSIS does. Addressing the Confederation Club in Kitchener on April 21, 1988, for example, he revealed that as a result of information provided by CSIS more than a dozen foreign diplomats have gone home after their intelligence activities were uncovered and several more have been permanently expelled as *persona non grata.** On May 5, 1988, in an address to the Kiwanis Club of Vancouver, he said CSIS carried out 50,000 security checks for the Calgary Olympics, and no terrorist slipped through the screening process. This too is information Canadians should have.

---

* After the end of the year under review, in June, 1988, a further example of such activity public. We have had a preliminary briefing and, after further investigation, will comment in next year's annual report.

10. Five Years Later

In recent years, Parliament has provided, in some of the laws it passes, that they shall be reviewed within a set period of time. Section 69 of the *CSIS Act* is an example of this practice. It calls for "a comprehensive review of the provisions and operation of this Act" by a Parliamentary committee in 1989, five years after it came into effect.

In a democracy like ours, Parliament does not deliberate in a vacuum. Behind the debates of 1983 and 1984 lay the work of the McDonald Commission from 1977 to 1981 and a public discussion that can be traced back at least to the 1960s. As the Parliamentary spotlight turns on the *Act* again, the public has a voice. Experts will make their views known. So will others with a personal or professional interest in security intelligence. The media will report various views--and likely put forward some of their own.

We too plan to play a part. As close observers of CSIS since its creation, with full access to its files and an extra-bureaucratic standing that lets us speak out clearly within the limits imposed on us by considerations of national security, we feel a responsibility to share what we have learned. We have already made some suggestions in past annual reports. Looking ahead to 1989, we will have specific proposals for amendments in next year's annual report.

But Parliament and the public will not want to enter the review process cold. So, setting housekeeping matters aside for the moment, we set out in this chapter some of the issues that we see. We generally phrase them as questions because we do not want to seem to close any options.

Security Intelligence and Public Policy

The collection of information and its translation into intelligence is intended to serve Canada's long-term strategic and policy interests. This is only possible if there is constant communication between those who develop policy and those who produce intelligence. Many authors have commented--not specifically speaking of Canada, rather of a common pattern in the Western world--that the consumers of security intelligence often do not know what is available or what could be produced while, conversely, the producers of security intelligence often do not know the issues on which the policy-makers need intelligence.

In Canada, the users of intelligence are as numerous as the arms of the government. They include the Cabinet and senior officials of all departments and agencies. There are also many producers of many kinds of intelligence--economic, foreign, military and security (see Appendix C of this Report). CSIS is only one player.

Another issue arises out of the excellent relations that CSIS--fortunately--bas with sister agencies in friendly countries. Since Canada's interests are similar to the interests of these countries, the intelligence that CSIS gets from them is mostly relevant to Canadian users. But CSIS must guard against adopting the outlook of these agencies at the expense of Canadian priorities.

In Chapter 6, we cite the Australian experience with an Office of National Assessment separate from the information gatherers in the intelligence agencies.

Should there be a new mechanism responsible for bringing intelligence of all kinds together before it is delivered to those who write policy and make decisions?

Security Intelligence and the Wider Community

A certain isolation from society as a whole is a fact of life for security intelligence services everywhere. For reasons of national security, an intelligence service cannot have frank exchanges with the private sector, politicians, educators, the news media--not even always with other arms of government.

Elsewhere in government the situation is quite different. Many officials have come to public service from successful careers in business, the professions, non-profit organizations, trade unions, the media and every other imaginable field. Specialized tasks are contracted out to experts. There is movement of personnel among departments and agencies. Public servants attend conferences where they exchange views and information with people in the private and voluntary sectors. In these and other ways, public servants remain integrated with society as a whole and have opportunities to keep abreast of developments in society.

Security intelligence officers, on the other hand, usually enter the field at an early age and stay with it until retirement. In Canada, CSIS officers are not covered by the *Public Service Employment Act*, so they are not "public servants" in strict legal terms. This means that rotation between CSIS and other arms of the federal government is, for all practical purposes, next to impossible. CSIS officers seek to guard their anonymity and stay away from places like conferences where the nature of their work might become obvious. For all of these reasons, CSIS forgoes many potentially fruitful exchanges.

Should the law be amended in such a way that the ability of staff to rotate between CSIS and other arms of the federal government is enhanced?

Would it be worth carrying out the extensive security clearances that would be required to allow outside experts to rotate through CSIS?

The Dissemination of Intelligence

The dissemination of intelligence under the control of CSIS is governed by section 19 of the *Act*, which does not contemplate disclosure outside government. We have already suggested (Annual Report 1985-86, page 45; Annual Report 1986-87, page 30), that there could be value in tipping individual Canadians when a voluntary organization they belong to is under, or risks coming under, clandestine foreign influence. It is not up to the Service to decide when members of the public should be told about foreign influence.

But it is not right that individual Canadians should, in all good faith, support and participate in the activities of foreign- influenced front groups whose covert objects are known to CSIS. Or that Canadian organizations with legitimate goals and methods should, in all good faith, become targets for infiltrators whose real aims as foreign agents are known to CSIS.

Should there be provision for some government body with authority to decide when CSIS should convey security intelligence to members of the public?

CSIS exchanges information with police and security agencies in Canada and abroad. We are told that care is taken to withhold intelligence from certain regimes that might make it a tool of oppression. However, CSIS has no comprehensive automated system for collating adverse personal information that it gives to police and other agencies. This is awkward for us, as we have an explicit duty under section 38 of the *Act* to monitor the provision of information to other agencies (see page 6).

Should there be an explicit requirement on CSIS to maintain statistical records of information passed to foreign agencies?

Threats to the Security of Canada

The cornerstone of CSIS's mandate is the definition of threats to the security of Canada, found in section 2 of the *Act*. Two expressions in that section need clarification:

- *Foreign influenced:* At the extreme, this is plain; there can be no doubt that a person who takes a hostile government's money under the table in return for pressing its views on the Canadian public is foreign influenced in a way that represents a threat to the security of Canada. But the Act surely does not contemplate the kind of foreign influence that colours the opinion and the talk of many, virtually all, Canadians--the subtle influence of foreign advertising, of foreign books, films and television, and so on.

- *Detrimental to the interests of Canada:* We have found uncertainty about the meaning of this term an issue in dealing with certain complaints. Is it "detrimental to the interests of Canada" simply to do things (a) without acknowledging publicly that one is (b) acting on behalf of a foreign power. Or is there a third specific condition--that (c) actual harm can be shown to be done. We have asked for an independent legal opinion on the meaning of this term.

  Should the terms 'foreign influenced" and "detrimental to the interests of Canada" be defined in the statute?

The Solicitor General has directed CSIS to use only non-intrusive techniques in its investigations under paragraph 2(d), which covers activities which have sometimes been referred to as "subversion". Any active investigation of these threats now requires the personal authorization of the Solicitor General. We have applauded these safeguards for lawful advocacy, protest and dissent (see Chapter 3, above). But they are only as strong as the commitment of the solicitor general of the day. What the present Solicitor General has ordered, a future solicitor general can rescind.

Should the requirement for special authorizations to investigate people involved in neither espionage nor terrorism be provided for in the statute?

Security Clearances

Section 42 of the *Act* provides for review (the new Government Security Policy uses the word "redress") where the deputy head of a department or agency denies federal employment to an individual or where a chance to sell goods or services to the federal government has been lost because an individual has been denied clearance.

But there are two situations in which an individual in the enterprise sector (whether public or private) has no access to effective review when an employment opportunity is denied because a clearance has been denied. One is where the individual is refused employment or is fired by a federal contractor to remove an obstacle to selling to the federal government.

The other is where no contract is involved. It is most easily explained with an example. Over the next few years, everyone with access to restricted areas in airports will require security clearance in which checks by CSIS play a key part. An airline pilot denied clearance will be unemployable. But no contract to supply goods or services to the federal government is involved. Rather, it is the airlines that use federal services. Yet the *Act* as now worded offers a pilot in this situation no effective review under section 42. The only avenues available would be a request for departmental reconsideration or an application to the courts.

We could hear certain aspects of such cases under section 41, which permits complaints "with respect to any act or thing done by the Service", but we do not consider this an adequate substitute for a section 42 complaint.

For one thing, section 41 adds a step to the process by requiring that a complaint first be addressed to the Director of CSIS. This is appropriate in most cases. Where CSIS has erred through inadvertance, say, it should have a chance to set the matter right on its own. But a recommendation to deny a security clearance is presumably a deliberate, careful decision that is not likely to be changed by the Director.

More important, there is no explicit provision in the *Act* for disclosure to the complainant under section 41. Generally speaking, this makes sense. In section 41 complaints, it is ordinarily the complainant who has the allegations and CSIS that puts up the defence. Security clearance complaints are different. As discussed in Chapter 7 above, we have a duty to advise complainants under section 42 of the allegations against them so they can make an informed response during our investigation. There are similar provisions for disclosure in citizenship and immigration cases.

> *Should there be a more effective remedy where an individual is denied employment with a private firm because a security clearance has been refused on the advice of the Service?*

The *Act* provides a remedy through our complaints process when there is "denial of a security clearance" (section 42). The word "denial" can be narrowly interpreted to mean “refusal". That would open a loophole, because the authorities could effectively refuse a clearance without risking a complaint by letting the application sit indefinitely in the In basket, never formally rejecting it. We would likely take the position that "denial" should cover "unreasonable delay" as well as explicit refusal.

Should "denial" be defined in the statute to include unreasonable delay as well as explicit refusal?

CSIS Operations

We have previously (Annual Report 1986-87, page 12) suggested that there might be value in making provision for emergency warrants. Getting a warrant is currently a 16-stage process. An elaborate process is in order. Limiting the use of intrusive powers is one of the keys to the *CSIS Act;* it should not be too easy for CSIS to get a warrant.

But sooner or later an operation is bound to be compromised because a warrant could not be secured quickly enough. We have sketched the scenario in which CSIS learns at the eleventh hour that a terrorist is stopping over briefly in Canada. An instant warrant might be needed so meetings that the terrorist held during the stopover could be monitored electronically. This is the kind of occasion when the current procedure might prove too cumbersome. We continue to gather statistics on the length of time it takes to obtain warrants following normal procedures.

The Director could be authorized, with the agreement of the Solicitor General in each case, to issue short-term, non-renewable warrants that would remain in effect just long enough to permit an application to the Federal Court--up to 96 hours, say. We would envisage an early report to our Committee whenever an emergency warrant was issued.

Should the Director, with the agreement of the Solicitor General in each case, be authorized to issue short-term warrants in emergencies?

Controls on Warrants

Since the "mid-course correction" announced by the Solicitor General on November 30, 1987, the Service's Warrant Review Committee has included a "devil's advocate"--a lawyer, responsible to the Deputy Solicitor General, with a mandate to argue against each warrant application. This is one of a number of improvements in the process (see Chapter 3).

But our original proposal (Annual Report 1986-87, page 9), was that the devil's advocate should argue before the Solicitor General (whose personal approval is required before CSIS can formally apply for a warrant) or the Federal Court (which grants or refuses warrants).

Having given the matter more thought in the intervening year, we now think that the Federal Court is the appropriate forum for the devil's advocate. This seems to us the best substitute for the usual principle of natural justice--the requirement to hear both sides of an issue *(audi alteram partem).* In security cases, the target obviously cannot be directly represented in court; it would defeat the purpose of a wiretap, say, if the target were warned through warrant proceedings.

Should statutory provision be made for a devil's advocate in warrant hearings? Should this official appear before the Federal Court?

Paragraph 21(4)(f) expressly gives judges of the Federal Court broad discretion to conditions into warrants. In practice, there seem to be certain specific conditions that judges consider in each case. They ordinarily protect privileged solicitor-client communications, for example, by:

- Prohibiting the interception of communications at the office or residence of a solicitor or at any other place ordinarily used by a solicitor for the purpose of consulting clients. (This parallels the protection found in the *Criminal Code* for warrants issued to police.)

- Restricting the interception of calls between a target and the target's solicitor (or an employee of the solicitor) to those that the Director of CSIS or a regional director general determine are related to the threat to the security of Canada specified in the warrant.

We discussed this issue in some detail in our 1986-87 Annual Report (pages 19-20). The question we raised then remains.

> *Should explicit statutory protection be given to confidential solicitor-client communications in security intelligence investigations?* Behind that question lies a second: *Should the statute include a checklist of limitations that judges of the Federal Court must consider when they grant a warrant?*

Oversight

Under subsection 39(3) of the *Act*, the only information that CSIS can withhold from us is cabinet confidences. As we have already noted, only in Australia does an independent body like our Committee have such wide access to security intelligence files. The secrecy surrounding cabinet confidences has not been a problem in our day-to-day work.

However, it clearly limits the scope of the oversight we provide. We have no way of testing the Service's performance against the demands that Cabinet has made on it. We have no way of knowing whether "problems" we identify flow directly from Cabinet orders.

Those of us who have been members of cabinets see no good reason for the lack of Committee access to relevant decisions of Cabinet or for insistence on cabinet secrecy in this case. The doctrine of cabinet secrecy is based on the need to let ministers disagree within the cabinet room, then present a united front when the debate is over. So the secrecy of cabinet discussion and the documents on which it is based is crucial to the principal of cabinet solidarity. But cabinet decisions must be revealed to those responsible for implementing them. Once a decision is made, it becomes known to public service employees. But not to us.

> *Should the Security Intelligence Review Committee have access to decisions* of *Cabinet relative to CSIS operations?*

Generally speaking, we rely on CSIS files for information. In the ordinary course of events, this is satisfactory. We have no reason to suspect CSIS of systematically trying to hide information from us. In an open society like ours, secrets have a way of surfacing eventually.

However, extraordinary circumstances could arise in which a member of CSIS felt it was necessary to bypass official channels to expose something believed to be wrong within the Service. We would hope that legitimate whistle-blowers would bring their stories to this Committee--in preference, especially, to telling them to the press. But the *Act* as written provides them no protection from discipline. In the United Kingdom, by contrast, a special official has been appointed to take "leaks" from members of the British Security Service ("MI-5") and investigate them. Members who provide information to this official are not required to identify themselves.

> *Should there be at least a statutory ban on prejudicial action against a member of the Service for conveying information to the Committee?*

Earlier in this Report (Chapter 3) we have said something of our protracted discussions with CSIS about the publication of warrant statistics. In this case we have come to a firm view:

> *Parliament should consider amending the statute so as to require the publication of specified warrant statistics.*

Access to Information and Privacy

We are not sure that the relationship between the *Access to Information Act* and the *Privacy Act*, on the one hand, and the *CSIS Act*, on the other, has yet been worked out with sufficient care. The Committee is, of course, aware of Parliament's report *Open and Shut* of March, 1987.

> *Should Parliament consider statutory amendments to reconcile access and privacy rights with the needs of national security?*

Basically Sound

Having raised all these matters, we should say that we believe the *Act* is basically sound. Most of the time and in most ways, it works well as a framework for carrying out the five basic principles articulated by the McDonald Commission:*

- The rule of law is paramount.
- The means of investigation must be proportionate to the gravity of the threat and the probability of its realization.
- The need for given investigative techniques must be weighed against the damage they might do to personal freedom and privacy or to valued social institutions.
- The more intrusive the technique, the higher the authority that must be required to approve its use.
- Except in emergencies, less intrusive techniques must be preferred to more intrusive techniques.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), pages 513--514.

A civilian agency whose mandate is spelled out in law rather than by executive order, with clear political and judicial control and independent review, remains the appropriate model for security intelligence in Canada.

Appendix A

Ministerial Direction to CSIS, 1987-88

1. Procedures for Ministerial Consultation
2. Ministerial Prerogative
3. Disclosure of Certain Types of Information
4. Conduct of Activities Involving Certain Foreign Authorities
5. Ministerial Review of Administrative Arrangements
6. (Repetition of earlier ministerial direction)
7. Interim Management Instructions
8. Implementation of Government Policy
9. Disclosure of Information on Ministerial Authority
10. Clarification of Ministerial Policy
11. Disclosure of Information to Canadian Authorities
12. CSIS Audit Activities
13. Retention of Information
14. Ministerial Notice in Relation to Administrative Matters
15. Retention of Certain Types of Information and Review of Operational Matters
16. Transfer of CSIS Equipment
17. Delegation of Authority
18. CSIS File Disposal
19. (Repetition of earlier ministerial direction)

Appendix B

Summary Case Histories of Complaints Dealt With by the Security Intelligence Review Committee, 1987-88

Security Clearances

1. Alleged Subversion: A clearance was denied on the grounds of dishonesty because the individual failed to disclose full particulars of his past involvement in an organization regarded by CSIS as subversive, refused to give CSIS the names of others involved in this organization and, finally, allegedly falsified documents about his education and personal history.

The individual admitted during the Committee's investigation that he made a serious error in judgement when he misled CSIS in an interview about the extent of his involvement in the organization concerned. He explained that he "panicked". He also admitted that he was not completely frank in answering questions on a job application form; the information he provided was true, but it masked his involvement in the organization concerned. CSIS brought no evidence to support its allegation of falsification of documents.

The activities that gave rise to CSIS's concern about this individual had ceased five years before, and he had renounced his previous beliefs. The individual made mistakes, but his explanations were credible and his evidence before the Committee was open and honest.

CSIS and the employer also erred in this case. The Committee completely rejects the notion that refusal to name others has any place in a CSIS recommendation against granting a security clearance. The employer did not, as it should have under the Government Security Policy, give the individual a chance to respond to CSIS's allegations before the clearance was denied.

The Committee concluded that the complainant would be unlikely to act in a way that would pose a threat to the security of Canada and recommended that he be granted clearance.

Citizenship

2. Terrorism: Citizenship was denied a landed immigrant because of a belief that he would engage in activities defined by paragraph 2(c) of the *CSIS Act* as a threat to the security of Canada--namely, "activities within ... Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within ... a foreign state".

CSIS presented compelling evidence that this individual was active in a terrorist organization. He admitted to criminal offences for which he had been convicted in Canada. There was no dispute, for example, that he had helped load an illegal shipment of arms. He tried to convince the Committee that he had become involved in this organization without realizing what he was getting into. But his vagueness and frequent memory lapses damaged his credibility.

The Committee found that denial of Canadian citizenship was justified because there were reasonable grounds to believe that this individual would remain a security threat.

3. Objection Withdrawn: Citizenship was denied to a landed immigrant because of his membership in an organization considered subversive by CSIS. As a result of change in the treatment of alleged subversion, announced by the Solicitor General on November 30, 1987, the objection to citizenship for this individual was withdrawn. The Committee thereupon closed its file. This individual has since become a Canadian citizen.

4. Objection Withdrawn: Except that it involves a different individual, this case is identical with the previous one in every significant detail.

5. Objection Withdrawn: In this case, CSIS withdrew its objection before the Committee began its investigation, so no details of the allegations are on the file.

Immigration

6. Criminality: A deportation order was made against a landed immigrant on the basis of criminal intelligence reports indicating that he was involved in organized crime.

The RCMP presented strong evidence from a variety of sources demonstrating the complainant's involvement in extortion and threats on behalf of a criminal organization.

The complainant gave no oral evidence, although he was repeatedly urged to take advantage of his right to be heard. In a written submission he denied his involvement in organized criminal activity, but he did not deal in a substantial way with any of the specific allegations. His counsel confined himself to challenging the Committee's jurisdiction and arguing that the Committee's procedures offended the *Canadian Charter of Rights and Freedoms.*

The Committee concluded that the deportation proceedings were justified.

7. Objection Withdrawn: An individual was denied entry to Canada because of RCMP allegations that he was involved in organized crime. But the RCMP withdrew its objection before the Committee began its investigation, so no details of the allegation are on the file.

Complaints under Section 41*

8. Alleged Harassment: An individual complained that there was no foundation to CSIS's suspicion that he had given Canadian secrets to a foreign government. He further complained that CSIS had investigated in a way that affected his physical and mental being as well as his professional reputation.

---

* In addition to the cases reviewed here, there were 30 complaints that were clearly out of the Committee's jurisdiction or in which the complainant offered no factual base on which an investigation could proceed. The complaints described here are those on which investigations were conducted and completed.

This individual had been seen taking money from a suspect official of the foreign government. The complainant, who was assisted by counsel, denied that he had betrayed Canadian secrets and he presented evidence to support his allegations of intrusive and illegal conduct by the Service.

The Committee concluded that CSIS had an obligation to carry out this investigation and that it had not made unreasonable or unnecessary use of its powers.

9. Payment of a Source: An individual who provided information to CSIS complained that he had not been paid as much as agreed upon. The dispute arose out of a misunderstanding. The Committee reviewed the situation and recommended a settlement. This recommendation was accepted by both parties.

Appendix C

The Intelligence Network in Canada

The Canadian Security Intelligence Service (CSIS) is part of a network of federal agencies concerned with security and intelligence. Except for the RCMP, it is the part best known to the general public; it is a key part; but it is, nonetheless, only a part.

This appendix briefly catalogues the major constituents of the network. It is based on a paper prepared in 1987 for members of the Security Intelligence Review Committee, to help them explore CSIS's mandate by placing it in the context of the work done by other agencies.* The Committee thought it would also be of interest to the public. Drastic trimming was required because much of the information in the original paper is secret. So the material presented here is by no means comprehensive. Much of it will be new to non-specialists, however.

The positions and agencies catalogued here are those that set priorities and that receive, produce, analyse and disseminate intelligence. By intelligence, we mean information in its finished form,** which provides a basis for government action. The protection of assets (referred to here as "security services") is touched on only incidentally.

It must be stressed that this catalogue is purely descriptive; no evaluation of the positions and agencies named can be read into it.

The Solicitor General

The Solicitor General is a central figure in the security intelligence network, responsible not only for CSIS but for the RCMP. He is assisted by the Deputy Solicitor General, by the Police and Security Branch within his Department and by the Inspector General.

With respect to CSIS, the Solicitor General has a number of responsibilities and powers under the *CSIS Act.* He issues written directions to CSIS on the conduct of both individual cases and entire classes of cases. His approval is required for each application CSIS makes to the Federal Court for a warrant to use such intrusive powers as wiretapping. His approval is also required for each agreement CSIS enters into with another agency--federal, provincial or foreign.

The Deputy Solicitor General assists and advises the Solicitor General. He coordinates the development of policy and is consulted extensively by the Director of CSIS. Under the direction of the Deputy Solicitor General, the Police and Security Branch initiates, develops and administers policies, operational directives and management systems on behalf of the Solicitor General. It also advises the Solicitor General on the activities of CSIS, the RCMP, federal and national law enforcement and counter-terrorism programs.

---

* The Committee acknowledges the generous assistance of many officials who provided information although they were under no obligation to do so.

** Analysts process raw information into intelligence by evaluating it for reliability and interpreting it to determine its meaning and significance. This is the stage in which processing (e.g., translation, photo interpretation, indexing) occurs as well as analysis.

You Get Letters ... A Glossary of Acronymns

ARG	-	Assessment Review Group; an ARG is a task force that reviews material prepared by a SARG before it is submitted to IAC.
CCSI	-	Cabinet Committee on Security and Intelligence.
CSE	-	Communications Security Establishment; Canada's signals intelligence agency.
CSIS	-	Canadian Security Intelligence Service.
EIC	-	Economic Intelligence Committee; an offshoot of IAC.
IAC	-	Intelligence Advisory Committee; with SAC, one of two principal subcommittees of ICSI; parent committee of EIC.
ICSI	-	Interdepartmental Committee on Security and Intelligence; a committee of deputy ministers that serves CCSI; its principal subcommittees are SAC and IAC.
IG	-	Inspector General; the Solicitor General's watchdog on CSIS.
NSEU	-	National Security Enforcement Unit; units within the RCMP that, among other things, ensure liaison with CSIS and with other police forces.
PCO	-	Privy Council Office; as the Cabinet secretariat, the nerve centre of government operations in all fields, including security and intelligence.
RCMP	-	Royal Canadian Mounted Police.
SAC	-	Security Advisory Committee; with IAC, one of two principal subcommittees of ICSI.
SARG	-	Specialized Assessment and Review Group; SARGs are IAC task forces that produce foreign intelligence reports as well as longer research papers on specific topics.
SIRC	-	Security Intelligence Review Committee; Parliament's and the public's watchdog on CSIS.
TARC	-	Target Approval and Review Committee; an internal CSIS body that decides who should be investigated and how intensively.

* Rare; the full name is commonly used.

Canadian Security Intelligence Service (CSIS)

The core mandate of CSIS is spelled out in section 12 of the *CSIS Act*--to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" and to "report to and advise the Government of Canada" on these matters.

CSIS's two major operational branches are Counter-terrorism and Counter-intelligence. An Analysis and Production Branch draws on information from the operational branches and from other covert and open sources to produce intelligence for use in many parts of the government. Another major program is security screening for public servants and others who have access to sensitive information and other assets vital to national security.

Important coordinating roles within CSIS are played by the Executive Committee, the Operations Policy Development Committee and the Target Approval and Review Committee (TARC).

Because much of CSIS's work must be done in secrecy, there are a number of controls on it. The role of the Solicitor General is discussed above. To use intrusive powers like wiretapping, CSIS requires warrants from the Federal Court of Canada. The *CSIS Act* also provides for monitoring by two external watchdogs--the Security Intelligence Review Committee and the Inspector General.

Inspector General

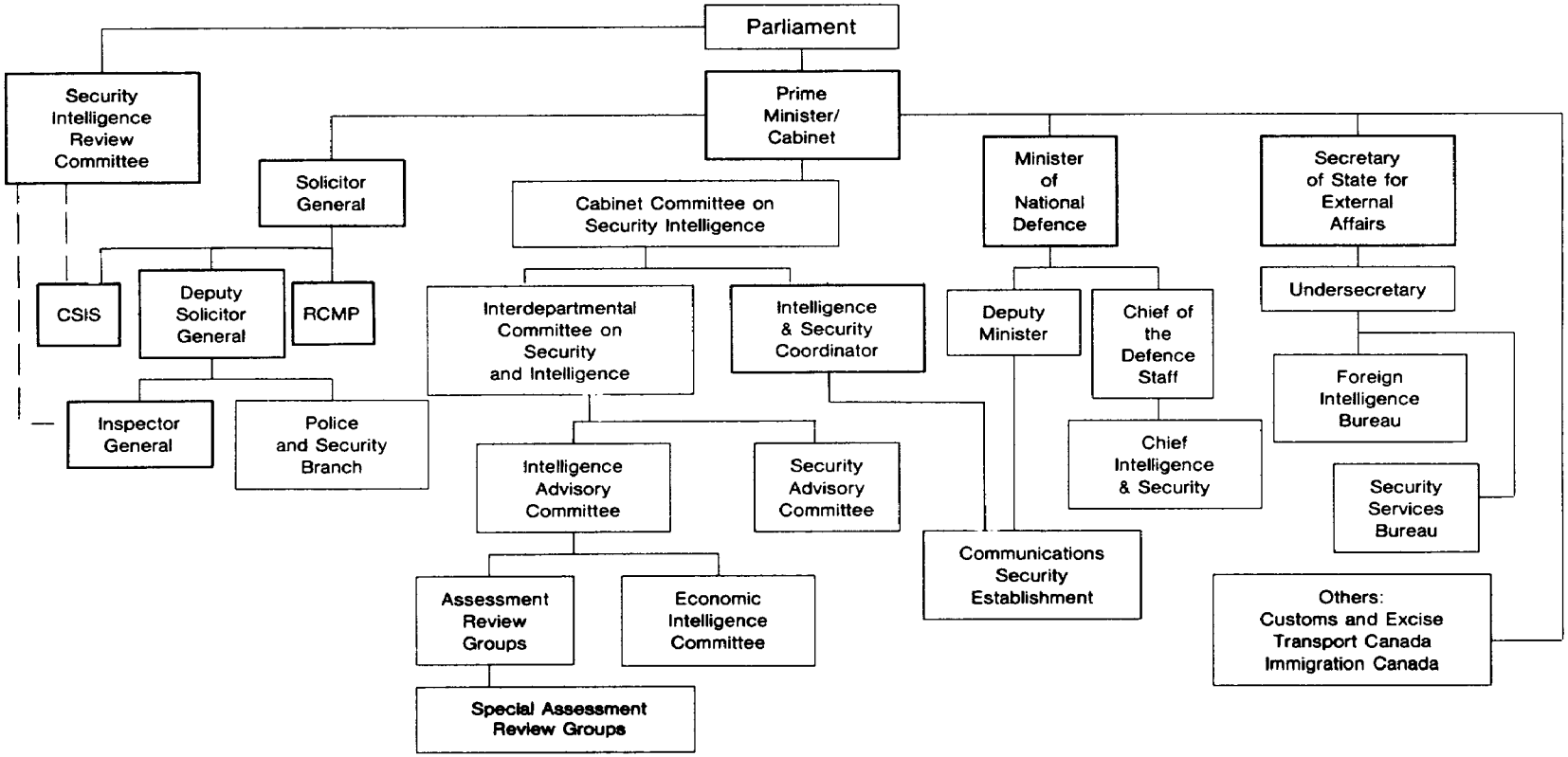
Reporting through the Deputy Solicitor General, the Inspector General is the Solicitor General's watchdog on CSIS, monitoring CSIS operations, policy, guidelines and internal controls. The Inspector General reviews the secret annual report that the Director of CSIS makes to the Solicitor General and issues a certificate stating (a) whether he is satisfied with this report, (b) whether the Service has remained within the bounds set by the *Act* and by the Solicitor General's instructions and (c) whether the Service has made "unreasonable or unnecessary" uses of its powers.

Security Intelligence Review Committee (SIRC)

SIRC is Parliament's and the public's eye on CSIS. It is composed of five part-time members appointed by the Governor in Council after consultations between the Prime Minister and the leaders of opposition parties recognized in the House of Commons.

The Committee has a dual mandate spelled out in the *CSIS Act*--oversight and complaints. In its oversight role, SIRC monitors CSIS's effectiveness with particular attention to ensuring that the Service does not make "unreasonable or unnecessary" use of its powers. SIRC also investigates complaints against CSIS and complaints about the denial of security clearances in public service employment, federal contracts, immigration and citizenship.

At a Glance . . . Major Components of the Intelligence Network



Notes: a) For simplicity's sake, only the most direct lines of authority are indicated.
b) Positions and departments with major statutory responsibilities are indicated by darker boxes.

SIRC's annual report is tabled in Parliament and is available to the public. Some of the special reports that SIRC makes to the Solicitor General on specific topics are also made public.

Royal Canadian Mounted Police (RCMP)

Part IV of the *CSIS Act* (the *Security Offences Act*) gives the RCMP primary responsibility for apprehending those who threaten the security of Canada or foreign diplomats in Canada. While CSIS pinpoints threats, the RCMP makes the arrests and assembles the evidence for the prosecution. The RCMP works closely with other police forces inside and outside Canada in carrying out this responsibility.

Through its National Security Enforcement Units (NSEUs), the RCMP exchanges information with CSIS and with other police forces on politically motivated crime, criminal activity by extremists, and other national security matters. NSEUs do not investigate specific offences but collect, coordinate and disseminate criminal intelligence. They are also responsible for issuing terrorist alerts and preparing threat assessments with regard to foreign diplomats in Canada and dignitaries from abroad visiting Canada.

The RCMP also provides a range of security related consultative and other protective services to senior officers of government, to foreign embassies and consulates, to dignitaries visiting Canada, at airports and elsewhere.

Transport Canada

The security of the national transportation system--on land and water and in the air--and its readiness to cope with emergencies is largely the responsibility of Transport Canada. The accent on airport security has risen in recent years because of frequent terrorist incidents in terminals and aboard aircraft in many parts of the world.

A Director General, Security and Emergency Planning oversees the work of four branches concerned with (a) policy and planning, (b) security operations, (c) intelligence, communications security and training and (d) emergency planning and the "Situation Centre" that would be the coordinator of operations in an emergency. The Director General is also responsible for the work of regional security directors.

Among other responsibilities, the Intelligence, Communications Security and Security Training Branch (a) coordinates the collection, analysis and dissemination of intelligence information from other agencies and (b) provides intelligence digests in support of departmental objectives as well as (c) providing threat assessments relevant to the protection of the national transportation system.

Employment and Immigration Canada

Immigration Canada's interests include (a) attempts by terrorists to use Canada as a haven, as a base of operations or for transit, (b) political and economic developments abroad that lead to international migration movements that could bring legal or illegal immigrants to

Canada and (c) immigration rackets, including the organized smuggling of people into Canada and the production, sale and use of fraudulent documents.

An Intelligence Division produces two kinds of intelligence, which it calls "strategic" and "tactical". Under the tactical heading, it develops and takes part in the development of programs for detecting fraudulent immigration practices--for example, distributing copies of newly-discovered forgeries to ports of entry so officials there will know what to look for. Strategic intelligence includes background briefing papers, immigration studies and trend analyses regarding enforcement/control activities and the development of recommendations for improving legislation, policy and procedures.

There is also a Security Review and Special Category Division whose work cannot be described here for security reasons.

Immigration Canada circulates an advisory notice to CSIS and other agencies on each application for a visa or for permanent residence in Canada, so they have an opportunity to raise any security concerns about the individual concerned.

Revenue Canada (Customs and Excise)

The security intelligence concerns of Customs and Excise are two-fold--"narco-terrorism" (drug trafficking aimed at raising money for terrorist operations) and illegal exports of defence and defence-related goods and technologies. Both these matters are dealt with by the Interdiction and Intelligence Division at headquarters and by Field Interdiction and Intelligence Units.

The headquarters Division gathers information on potential risks, the methods and routes used by offenders and other matters, and it produces both tactical intelligence for use in the field and strategic intelligence for senior management's use in planning. It liaises with the customs services of other countries, with law enforcement agencies in Canada and with such international agencies as the Customs Cooperation Council and Interpol.

Under the Export Control Program administered by this Division, export shipments are inspected to ensure that strategic goods and technologies are not being exported contrary to the *Export and Import Permits Act.*

Department of External Affairs

The Department has a Security Services Bureau whose responsibilities include developing and formulating policy for international cooperation against terrorism as well as providing a range of security services.

The Department of External Affairs has a Foreign Intelligence Bureau which collects and analyses information as a basis for providing intelligence to the Intelligence Advisory Committee (described below) as well as within the Department.

The Bureau has separate divisions for political and economic intelligence. Analysts are assigned on a regional basis (e.g., Middle East) or to global issues (e.g., nuclear proliferation). A third division interviews selected immigrants, defectors and Canadians who have lived in closed societies, to glean useful information not available from open sources. Such interviews are conducted only with the consent of the subject. The fourth division provides support for the rest of the Bureau.

Department of National Defence

The Chief, Intelligence and Security is responsible for the collection, production and dissemination of defence intelligence, including scientific and technical intelligence, for the Canadian Forces. A Director General, Intelligence and a Director General, Security report to the Chief. The Director General, Security is responsible for security services in the Department and the Forces.

Under the Director General, Intelligence are five directorates--(a) Defence Intelligence, (b) Current Intelligence, (c) Imagery Exploitation, (d) Scientific and Technical Intelligence and (e) Intelligence Plans and Doctrines. The Director General, Intelligence also maintains contact with intelligence agencies in other countries.

Communications Security Establishment (CSE)

CSE has a twin mandate--signals intelligence and the security of communications and data processing in federal agencies.

CSE provides a service of signals intelligence in support of Canada's foreign and defence policies based on the collection of foreign radio, radar and other electromagnetic transmissions, and it distributes reports on what they reveal. It is responsible to the Minister of National Defence.

CSE's communications security role is to help federal agencies prevent unauthorized access to their telecommunications and electronic information processing. CSE also provides cryptographic key material and documentation to departments and agencies.

Coordinating Committees

There are a number of direct links, formal and informal, among the various security and intelligence agencies. In addition, a series of committees is in place to provide coordination.

Cabinet Committee on Security and Intelligence

At the centre of Canada's security intelligence network is the Cabinet Committee on Security and Intelligence. It is headed by the Prime Minister personally. Among its members are ministers whose departments (a) make significant use of foreign and security intelligence, (b)

are major gatherers or producers of intelligence or (c) are responsible for security operations. This Committee sets policy and determines the Government's security and intelligence priorities.

Privy Council Office (PCO)

In this as in other domains, the Prime Minister and Cabinet are supported by PCO, which includes a Security and Intelligence Secretariat headed by the Intelligence and Security Coordinator responsible for (a) interdepartmental coordination and (b) ensuring that the Prime Minister and the Cabinet Committee get the information and advice they need.

Interdepartmental Committee on Security and Intelligence (ICSI)

ICSI (pronounced "ick'-see") is headed by the Clerk of the Privy Council and includes deputy ministers of departments that are either major producers or major users of intelligence (or both), the Director of CSIS and the Commissioner of the RCMP.

Its responsibility is to develop proposals for the Cabinet Committee on Security and Intelligence. It has two principal subcommittees--the Security Advisory Committee (SAC) and the Intelligence Advisory Committee (IAC).

Security Advisory Committee (SAC)

SAC is concerned with security matters which affect federal government departments. The Committee, on which CSIS sits as a member, is chaired by the Deputy Solicitor General. SAC is supported by a small secretariat.

The Committee has a role in formulating security policy that has interdepartmental scope. It advises ICSI on security requirements and priorities. It carries out some of its functions through sub-committees which study specific issues, such as protection of information and property and counter-terrorism.

Intelligence Advisory Committee (IAC)

The IAC reflects the collective Canadian intelligence community. As such, the IAC members cooperate and coordinate the production of intelligence, drawing on research and analysis carried out by federal agencies, notably CSIS, the Department of External Affairs, the Department of National Defence and the Communications Security Establishment. Analysts meet in task forces called Special Assessment Review Groups (SARGs). Documents produced by SARGs are then reviewed by the Assessment Review Groups (ARGS) before being presented to IAC for final approval and dissemination.

The IAC chairman is the Intelligence and Security Coordinator in the Privy Council Office. CSIS is represented by the Director, with a designated alternate at the Deputy Director level.

An important subcommittee of IAC is the Economic Intelligence Committee (EIC), which directs the production of economic intelligence for IAC. CSIS is also represented on this subcommittee.

IAC also advises ICSI on policy issues such as intelligence needs and the coordination of intelligence programs and plans.

Appendix D

SIRC Staff on July 1, 1988

Maurice Archdeacon, Executive Secretary	990-6839
Danielle Blache, Senior Secretary	990-8442
Annie Demirjian, Executive Assistant	990-6319
Shirley Heafey, Senior Complaints Officer	993-4263
Arthur Graham, 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
Madeleine DeCarufel, Administration Officer and Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, Records Clerk	998-5258
Diane Marion, Receptionist-Secretary	990-8441