SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1991-92

Canada

Security Intelligence Review Committee
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

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

Cat. No. JS71-1-1992
ISBN 0-662-59274-3

The Honourable Doug Lewis, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Lewis:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1991-92, for submission to Parliament.

Yours sincerely,

John W.H. Bassett, P.C., C.C., O.Ont.
Chairman

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

E. Jacques Courtois, P.C., Q.C.

Stewart D. McInnes, P.C., Q.C.

Michel Robert, P.C.,Q.C.

Contents

The Security Intelligence Review Committee at a Glance

The Security Intelligence Review Committee (called ``SIRC'' or ``the Committee'' in this report) acts as the eyes of the public and Parliament on the Canadian Security Intelligence Service.

The Canadian Security Intelligence Service (CSIS) is a federal government agency created in 1984 by the *Canadian Security Intelligence Service Act* (the *CSIS Act*). CSIS investigates terrorists, agents of hostile intelligence services and others whose activities may be a ``threat to the security of Canada''. CSIS must protect its sources and methods. Much of its work must therefore remain secret. This makes it difficult for politicians and the Canadian public to ensure that CSIS operations are effective and that at the same time CSIS respects the rights and freedoms of Canadians. To remedy these problems, the same law that created CSIS created SIRC.

The Committee is independent of the Government. The *Canadian Security Intelligence Service Act* provides that its five members are appointed by the Governor in Council after consultation among the leaders of all parties having more than twelve members in the House of Commons. Individuals may be appointed to the Committee only if they are already Privy Councillors or are appointed to the Privy Council for that purpose by the Governor General.

To the extent that national security permits, the Committee reports to Parliament through its annual reports. These are available to the public. They constitute a ``report card'' on CSIS operations that would otherwise not be allowed to come under public scrutiny because of national security considerations.

The Committee also has the power to investigate complaints relating to CSIS. First, it can investigate complaints by a person about ``any act or thing'' done by CSIS. It is not necessary that the person complaining be personally affected by what CSIS did. Second, the Committee can review certain denials of security clearances affecting federal government employees or job applicants or persons who seek to sell goods or services to the federal government under contract. In a related vein, it can also review adverse security findings that would affect a person's right to immigrate to Canada or obtain Canadian citizenship. If the Committee finds a complaint justified, it recommends a remedy.

1. Introduction

The SIRC Mandate

At approximately the same time as this report is being made public, the Review Committee will be coming to the end of its eighth year as the ``watchdog'' of CSIS. We think it would be appropriate, therefore, to review progress over the last few years and to publicly explain our interpretation of our mandate and our philosophy in carrying it out.

We can define our role in one pithy if somewhat ungrammatical sentence:

> To ensure that CSIS does things right and does the right things.

In the early years of this Committee's mandate, CSIS acted to a great extent as if it were simply a continuation of the RCMP Security Service. Despite public assertions to the contrary, SIRC found that most CSIS targets, policies, and procedures were virtually unchanged from those of the Security Service, and that CSIS' preferred source of recruits was still the RCMP. It took over three years for this state of affairs to change significantly.

Those who have followed the progress of CSIS with interest have seen our Annual Reports change from being compendiums of direct and implied criticism, in the early years, to being much more supportive accounts of CSIS' activities in recent years.

This progressive but clear-cut change in the tone and substance of our Annual Reports simply reflects the fact that CSIS is now virtually a new organization, hardly recognizable any more as the direct descendant of the Security Service of the RCMP.

The number and type of CSIS targets, the rigorous justification required before anyone or any group is designated as a target, the lucidity, logic, and balance of warrant affidavits submitted to the Federal Court, and the tone and content of reports by Intelligence Officers on targets' files have all changed significantly for the better.

Security considerations sometimes make it difficult for us to provide enough details of CSIS activities in our Annual Reports. We have the same difficulty as the Rt. Hon. Lord Justice Lloyd, the Commissioner who reviews MI-5 in England. He expresses our problem exactly when he says in his annual report:

> The task of reassuring the public would have been easier if I could publish everything. . . . I could then give chapter and verse. But for obvious reasons I cannot do that. I can only attempt to reassure in general terms.

As last year's report, and this one, demonstrate, we still have criticisms to make. Some we make publicly. Others, because of the nature of CSIS' work, we make privately to the Director and the Minister. But our criticisms are no longer based upon strong and fundamental disagreements with the CSIS view of the world. They are far more the results of differences of opinion regarding the

day-to-day implementation of CSIS policies than, as in the past, our opposition to those policies themselves.

CSIS might have moved in the right direction even if SIRC had never been created, but we believe that the Committee's public (and strong private) criticism of CSIS policies and procedures from 1984 to 1988 led to many of the most substantive changes in the Service's policies and practices.

We believe that CSIS management intends to work strictly within the letter and the spirit of the *CSIS Act* and Ministerial directions. However, the very fact that SIRC exists and that it reviews the activities of CSIS incessantly has an added salutary effect on the way the Service views each and every operation it undertakes. We have found, as we conduct our audit and review function from year to year, that our questions often lead to changes in CSIS activities even before we complete our final reports.

We believe that if SIRC and CSIS management have fulfilled their respective roles in a reasonably competent fashion over the last eight years, then it follows that the Service should, by now, be operating in a legal, ethical, and appropriate manner. And, generally, we find this to be the case; though, as mentioned earlier, we still have criticisms to make and improvements to suggest.

Continued vigilance by management, however, as well as the continued presence of SIRC (or some other similar body) is essential if Canadians wish to be sure that CSIS never again reverts to the habits that seem to plague, time and time again, every secret agency that does not have an effective external review process.

Complaints

The second principal role of this Committee is to deal with complaints from Canadians or legal residents, and to respond to reports from Ministers in immigration and citizenship cases involving security or criminal concerns.

Complaints about the denial of security clearances have declined from a flood in 1985 to a tiny trickle this year. We hope that this has something to do with Parliament's establishment of SIRC as an avenue for the appeal of such denials, but, whatever the reason, the change is welcome. Far fewer Canadians now find their careers arrested and their lives disrupted by the denial of a security clearance.

The attention given the Supreme Court decision in *Thomson* (see Chapter 6 for details) put this improvement in some jeopardy. As Mr. Justice Cory stated for the majority:

> The Committee's recommendation constitutes a report put forward as something worthy of acceptance. It serves to ensure the accuracy of the information on which the Deputy Minister

makes the decision, and it gives the Deputy Minister a second opinion to consider.

This means that potential complainants have to consider the fact that the emotional and financial costs of an appeal to SIRC could prove to be valueless even if the Committee came down strongly on the side of the complainant; the final decision being in the hands of the person who had decided to deny the complainant a security clearance in the first place.

Because we were very concerned that the ``appeal'' mechanism established by Parliament could now be seen as less worthwhile by persons denied a security clearance, we made a proposal to the Solicitor General of Canada which would have improved the situation without recourse to the best solution of all: an amendment to the Act. Our proposal is included as Appendix F to this report.

The Solicitor General's response to our proposal and the Chairman's acknowledgement are attached as Appendix G to this report. Clearly, the Minister's response does not go very far in providing the remedy we proposed. We acknowledge the Minister's proposal, and we certainly hope that the consultation process, and the requirement to inform us of the final decision, will be implemented with the full intention by all parties to provide the fairest possible result to the individuals concerned. In particular, we trust that the Deputy Minister's advice to us will include the basis for the decision not to accept our recommendation.

The End of the Cold War

Finally, one of our priorities over the next few years will be to ensure, on behalf of Parliament and the Canadian people, that CSIS is ``doing the right things''.

The end of the Cold War has removed much of the enormous threat that has hung over us for forty years. The threat of conventional or nuclear war with the Warsaw Pact has now almost entirely disappeared. Bureaucracies in such circumstances tend to seek other goals. We do not assert that CSIS is doing this now and, in any case, there is still a dangerous terrorist threat to guard against in the modern world. In March 1992, the Director established a task force to conduct a fundamental review of the mandate of CSIS (see Chapter 9 for details). We have been asking questions of CSIS for the past 18 months and we will carefully examine its conclusions about its revised role in a changed world.

2. Air India

At 07:14 a.m. GMT on June 23, 1985 Air India flight 182 from Montreal to London crashed into the sea off the coast of Ireland with the loss of all 329 persons on board, most of whom were Canadians. On October 4, 1991, the Committee announced that with the agreement and support of the Minister of Justice and the Solicitor General, we would proceed with our own review into CSIS activities before and after the crash. This study has been ongoing since that time and we will shortly submit a detailed section 54 report to the Solicitor General.

Our report is a long one and much of its content must remain classified. This chapter sets out, to the extent possible, our principal findings and conclusions.

(a) The Objectives and Our Methods

Despite the failure to date, to find any physical or other evidence to confirm the exact cause of the disaster, we undertook our study on the assumption that the aircraft was destroyed by an explosive device placed on board the aircraft at some time while it was in Canada. On the basis of the information we have seen, we believe that our assumption is reasonable; as is our other assumption that the disaster was a consequence of the ongoing dispute between Sikh extremists and the Government of India over the establishment of an independent Sikh country in what is now the Indian State of Punjab.

Our objective was to learn what information CSIS possessed about any threats of terrorist action against Air India or other Indian interests in or relating to Canada prior to June 23, 1985, and whether it fulfilled its mandate to investigate such threats and to advise the appropriate government and law-enforcement agencies in a timely and comprehensive way.

We also wished to learn whether CSIS assisted government and law enforcement agencies by providing, to the extent possible under its mandate as an intelligence gathering organization, all information and intelligence in its possession relevant to the criminal investigation of the disaster. As an adjunct to our primary objectives, we wanted to determine whether CSIS complied with all policies relating to the collection and retention or erasure of audiotapes. Also, we reviewed whether CSIS policies or prevailing practices governing the collection and processing of those audiotapes ensured that all information relevant to the disaster was evaluated for its intelligence value or its significance for any criminal activity and that no valuable information was lost.

As a final objective, we sought to determine if CSIS had any information or intelligence pointing to the involvement of any agency or representative of a foreign government being implicated in the destruction of the aircraft.

We reviewed many thousands of CSIS documents as part of this inquiry. We also conducted interviews of numerous personnel who were involved in the CSIS activities relating to the investigation of Sikh extremism before and after the disaster. We met with representatives of the families of the victims and officials of the World Sikh Organization and we invited them to make any presentation they wished regarding the disaster and its investigation.

Our inquiry was naturally restricted to the activities of CSIS in the matter, as we are not permitted under our mandate to pursue inquiries into the activities of other agencies responsible for the protection of civil aviation in this country or with the investigation of the disaster after the fact. The fact that this review is directed only at CSIS, therefore, should not be given any other interpretation.

Notwithstanding that our mandate is restricted to CSIS, the Commissioner of the RCMP kindly responded in a full and frank way to our request for a briefing on a number of issues relating to our inquiry. Our requests to the Force for information have similarly been acted upon. We have had to be particularly careful in this chapter to avoid any reference to matters the disclosure of which could jeopardize the still active RCMP investigation of the disaster. The Department of Justice also provided us with a useful briefing in response to our questions.

(b) CSIS Investigation Prior to the Disaster

Prior to June 1984, isolated acts of violence associated with Sikh protests against perceived injustices by the Indian Government caused little real concern to the police and security agencies here and the investigation of any threat from Sikh extremism was given a low priority. In June 1984, however, the Indian Government's occupation of the Sikh Golden Temple at Amritsar aroused fears of a major violent reaction from the Sikh community in Canada. These initial fears were allayed when it became apparent that the vast majority of Sikhs, while shocked and outraged, limited themselves to lawful demonstrations.

Small groups of hard-core Sikh militants were emerging in Canada and elsewhere, and the threat of violent acts by them was one of the first concerns to be faced by CSIS when it was established in July of 1984. Compared to some other, more recently active and dangerous terrorist groups at the time, the threat was not a major one and we found that the resources applied by CSIS to Sikh extremism were very limited and the priority for investigation remained low. CSIS investigators had not acquired a comprehensive understanding of Sikh extremism and its objectives.

By the Fall of 1984, CSIS had identified several of these extremist groups in Canada. These organizations had small followings in British Columbia and in southwestern Ontario, as well as elsewhere in Canada. Targeting authority was issued and principal members of the organizations were identified and actively investigated. Up until the time of the disaster, CSIS issued numerous threat assessments to the RCMP and other government agencies indicating a high level of threat

from Sikh extremists. These assessments, while accurately reflecting the information in the possession of CSIS, provided little intelligence on the nature and form that any threat activity might take.

Following the assassination of Indian Prime Minister Indira Gandhi at the end of October 1984, CSIS was further concerned that serious violence would erupt between the Hindu and Sikh communities in Canada, but this never materialized.

With the approach of the first anniversary of the assault on the Golden Temple and the planned visit of Rajiv Gandhi to the United States in early June 1985, CSIS intensified its investigative efforts, although no significant additional resources were applied to the targets. A plot to assassinate Rajiv Gandhi was uncovered in the United States just prior to his visit there and the persons arrested were linked to members of one of the Sikh extremist groups in Canada.

Despite initial fears, however, both the anniversary of the Golden Temple assault and the visit of Rajiv Gandhi passed without significant incident. Although CSIS still considered the threat to Indian interests in Canada from Sikh extremists to be high, some of the serious concerns of the previous month were lessened when Rajiv Gandhi safely departed from the United States. Just seven days later, Air India Flight 182 was destroyed.

(c) What Happened?

At 6:19 a.m. GMT on June 23, 1985, a piece of luggage being transferred from CP Flight 003 to an Air India flight at Narita Airport in Japan exploded in a baggage cart, killing two baggage handlers. Less than one hour later, Air India Flight 182 crashed into the sea off the coast of Ireland.

In the subsequent criminal investigation, attention centred on information pointing to the fact that on June 22, 1985, baggage had been deposited at Vancouver International Airport for two persons, both identified as M. Singh and L. Singh. One of these was to travel to Narita Airport in Tokyo by CP Air Flight 003, while the other was to travel to Toronto via CP Air Flight 060 where he would transfer to the Air India Flight 182. Investigation revealed that neither passenger occupied the seat allocated to him and there is no record that either boarded his flight. The unaccompanied baggage of these two individuals was loaded onto the flights, however, and it is assumed that the bag bound for Toronto was transferred to the Air India aircraft.

(d) What Did CSIS Know?

We examined all of the information CSIS had in its possession prior to the disaster that related to the investigation of possible Sikh extremist violence, particularly in the British Columbia

Region, and we also interviewed investigators and supervisors directly involved in the investigation.

The principal concern in the weeks preceding the disaster was for the safety of Rajiv Gandhi in the United States and the safety of Indian diplomats and missions in Canada. What information there was relating to threats to Air India seemed to focus on the possibility of hijacking or direct assault rather than bombing.

At the beginning of June 1985, CSIS placed a leader of a Sikh extremist group, who was later to become one of the principal suspects in the case, under physical surveillance. The Service continued to monitor his movements until June 17, 1985. The Prime Minister of India had departed from the United States on the day before.

The intelligence that CSIS possessed about the Sikh extremists prior to the disaster consisted mostly of information derived from the technical (discussed below) and physical surveillance of this one target; reports from friendly intelligence agencies; and warnings from the Indian Government. CSIS knew quite a lot about the identities and movements of the extremist groups and their members but to that time, little about their intentions or their potential for terrorist activity in Canada.

We could find no information that specifically pointed to an attack being planned against the Air India operations other than in some warnings originating from the Government of India (discussed below). We did, however, see CSIS reports emanating from some sources in early June 1985 that something big or spectacular was about to happen. CSIS used these reports to prepare a general threat assessment on June 18, 1985 which was comprehensive and which included information on several disturbing developments in Sikh extremist activity. Perhaps reflecting the dearth of intelligence in the area, however, the assessment provided little intelligence on the strength and capability for terrorist action of the hardcore extremists, or on the range of their possible targets.

One event that subsequently added a significant perspective to these reports occurred on June 4, 1985. Physical surveillance of the principal Sikh extremist target, revealed that he travelled from the B.C. mainland to Vancouver Island and met with Inderjit Singh Reyat, later to be convicted of offences related to the bomb explosion at Narita Airport. The two, accompanied by another person, then drove to a remote area and conducted what was at first believed by the surveillant to have been a one-shot discharge of a rifle.

CSIS investigators advised the RCMP of the event on the following day. It was only after the disaster, however, that a careful search of the area by the RCMP revealed evidence of an apparent test detonation of an explosive device having occurred at the site. We saw no document indicating that CSIS had conducted any immediate and comprehensive analysis of this and other information in an attempt to assess the capabilities and intentions of the two individuals.

Several other pieces of information possibly touching on the intentions of the principal target and his group were not to become available until after the disaster. These originated in the Punjabi content of the recorded telephone conversations of the target which occurred in the days and weeks prior to June 23, 1985, and which were not translated and available to investigators until weeks and even months after that date.

(e) Government of India Warnings

There has been much speculation about warnings issued by the Government of India that should have alerted CSIS to the fact that the aircraft was going to be attacked. We examined very closely the warnings that CSIS received in this regard in the first half of 1985. We found that without exception, these warnings were initially presented to the Department of External Affairs or to the RCMP and not directly to CSIS. These were the appropriate channels at the time. While several warnings were specific as to the threat, i.e. hijacking, and to the flight number and date, none referred to the flight that was destroyed and none of these particular threats materialized.

The Government of India did formally request, however, that additional security be provided to their aircraft and operations during the month of June 1985. CSIS was asked by the RCMP to provide a threat assessment on the basis of this warning and the RCMP was advised on June 6, 1985 that the threat to Indian interests in Canada, including Air India, was high but that CSIS had no information indicating any specific threat to the airline.

We were unable to find anything in any of the many warnings we saw issued by the Government of India, either specifically referring to Air India or to other more general threats, that would have provided an intelligence lead enabling CSIS to predict the attack on the doomed aircraft.

(f) Events After the Disaster

Understandably, CSIS was not immediately in a position to respond to the intelligence demands following the disaster since few investigators except those already directly involved in the investigation of Sikh extremism were in any way knowledgeable about the principal targets or about Sikhism and its dispute with the Government of India. The dramatic increase in personnel assigned to the investigation of Sikh extremism created initial problems of familiarization. We found, however, that there was immediate and full cooperation with the RCMP and a free exchange of information took place between the two agencies. Liaison arrangements were established at HQ and at regional offices.

We looked for any evidence of conflict or lack of cooperation between the RCMP and CSIS and found that while there were personality differences that arose from time to time, these did not have any serious consequences. Also, we noted that some activities of both CSIS investigators and

members of the RCMP were seen as encroaching upon the responsibilities of the other agency, again, with no serious consequences.

We noted one serious dispute that did occur after the disaster which involved an acrimonious exchange between two senior officers of the agencies that included an RCMP allegation that CSIS was acting in an area that was within the criminal investigation responsibilities of the RCMP. It appeared to be an isolated clash based to some extent on a misunderstanding and had no long term effect on the ongoing cooperation between the two agencies.

In seeking a cause for these problems we found that despite early concerns when CSIS was established that responsibilities regarding terrorism might overlap, CSIS policies detailing its relationship with the RCMP on cases involving security offences had not been developed. Early instructions issued from CSIS HQ to the regional offices failed to rectify this shortcoming. We noted as a consequence, indications that even the mandated role of CSIS in respect to the investigation was not clear to all personnel. One former senior officer told us that while the role was well understood by senior personnel, he was concerned that some CSIS investigators would conduct their inquiries as though they were criminal investigators and would compete with the RCMP to solve the case.

Other former senior officers, including the first Director of CSIS, did not share this concern. In the event, we saw no early instructions from CSIS HQ that attempted to clarify the CSIS mandate vis-à-vis the RCMP criminal investigation or which set out CSIS policy regarding the sharing of information and intelligence with the RCMP. We consider this to have been an unfortunate oversight on the part of senior management.

As the investigation progressed, RCMP officials felt it necessary to examine CSIS files on certain Sikh extremist targets in more detail. CSIS, whose mandate it is to collect intelligence and not evidence, was at first reluctant to expose its files, and by extension its methods and sources, for any evidentiary use by the RCMP. Lengthy negotiations took place between the two agencies, but eventually the RCMP investigators were allowed access to the files subject to some mutually agreed conditions on the subsequent use of the information.

Overall, we found no evidence that access to available CSIS information relevant to the RCMP investigation of the disaster was unreasonably denied to the Force.

A serious issue later arose, however, over the fact that in accordance with its established policies, CSIS had already erased three-quarters of the 200 or so audiotapes of the principal target's conversations recorded before the disaster and so these were not available to the RCMP for their requested examination.

(g) The Erased Audiotapes Issue

We found that in the Spring of 1985, as part of its investigation into Sikh extremism in the British Columbia Region, CSIS obtained a warrant to intercept the private communications of the leader of one of the Sikh extremist groups, who was later to become one of the principal suspects in the case. We looked into the erasure of certain audiotapes collected by CSIS between March and July 1985 as the product of the warrant. Central to the issue were concerns that important information might have been lost through these erasures.

CSIS affirmed that the tapes were erased in accordance with their policies and the Government's intention that such material should not be retained unnecessarily. We examined the CSIS policies to assess their appropriateness and the level of compliance.

CSIS Policies in 1985. Our review showed that CSIS had not yet developed its own policies in 1985 relating to the handling and processing of telephone intercepts recorded on audiotape. CSIS employees relied on different sets of policy and instructions governing retention or erasure which were developed and used earlier by the RCMP Security Service. The criteria for the retention of tapes were based on outdated terms having no defined meaning under the *CSIS Act*. This appears to have created confusion among the CSIS personnel who knew of the policies. Most employees involved with the collection and analysis of taped intercepts, however, were found to have had little or no understanding of the policies or even to have known of their existence. Importantly, few appeared to have been aware of the criteria and procedures for retaining a particular audiotape.

To compensate, the CSIS investigators and their technical colleagues relied on oral instructions or accepted practices from the past. These practices contained flaws that were not uncovered until the Air India tragedy prompted a closer examination.

From our review of the chronology of events and issues relating to the handling and processing of the Sikh extremist audiotapes, we found that the CSIS policies and procedures governing the retention and erasure of audiotapes existing at the time of the Air India disaster were seriously deficient in relation to accounting records and responsibility for decisions.

We believe two instructions were important in relation to the erasure of the Sikh leader's tapes. Three months before CSIS came into being, an instruction was issued which removed from Service facilities the capacity to collect and preserve criminal evidence tapes. This instruction was consistent with the provisions of the *CSIS Act* establishing the Service as an intelligence agency with no police powers or responsibilities.

The second document, from a less senior manager, instructed the CSIS Regions to retain tapes containing incriminating passages for one year to assist in the preparation of affidavits to renew warrants where this was considered necessary. The Regions, for reasons which are not clear, chose to ignore the instruction. While this instruction would have lowered the existing criteria

for retention, compliance, at the very least, might have enhanced investigator awareness of the option to retain tapes.

Chronology of Events. The telephone wiretap on the Sikh extremist leader was activated in March 1985, before the CSIS office in Vancouver was able to obtain the services of a Punjabi speaking translator. As the Service had difficulty finding a suitable translator, arrangements were made as a temporary measure to have the tapes translated in Ottawa. These arrangements soon broke down and by the time an on-site translator was obtained in early June, the B.C. Region investigators had been able to review only the tapes recorded to the beginning of April 1985, and a backlog of about 100 unprocessed tapes in which only the English language portions had been transcribed, had built up just prior to the disaster. We noted in this regard, that there was an apparent lack of serious concern by CSIS management over the long delays in the processing of these tapes.

A residual backlog of more than 80 tapes, which were recorded in April and early May, was not eliminated until late September and early October of 1985. Of these, only 50 tapes, which were translated by an RCMP official and thus deemed by CSIS not to have been assessed for intelligence purposes, were not subsequently erased in accordance with existing policy. Four others, retained for technical purposes, also survived.

On November 13, 1985 the RCMP asked CSIS for an accounting of all the tapes to that time related to Sikh extremists. The B.C. Region stated that almost all of their tape holdings prior to November 4, 1985 had been erased in accordance with CSIS policy. On February 7, 1986 the Department of Justice asked CSIS to retain all tape intercepts related to Air India. By this time, all tapes recorded since March 27, 1985, except for the 54 mentioned above, had already been erased. A claim by the RCMP that CSIS had been requested, in late June 1985, to retain all of the tapes from that date could not be substantiated.

The survival of fifty four of the 200 or so tapes recorded before the disaster was important in that it allowed the RCMP to analyze their content and determine that they contained no significant criminal information. The guarded way in which the recorded conversations were conducted also tended to reinforce the CSIS position that the other tapes already erased contained nothing significant.

In 1985 there were no clear guidelines for accountability. Discrepancies in the documentation make it impossible to obtain a definitive number of the tapes recorded by the Service from March to July 1985. The CSIS estimate is that there were 210 tapes recorded during this critical period.

We looked to see if it was likely that this lack of an accounting system resulted in any audiotapes being erased before being processed. As the accounting records for the processing of the Sikh extremist leader's tapes are fragmentary, it is now impossible to say with certainty that no unprocessed tapes were erased.

In conclusion, we found there was an absence of appropriate policy and clear guidelines as to who should decide whether an audiotape was to be retained or erased. There was confusion in CSIS' ranks on this issue and on the meaning of the retention criteria. In the case of the Sikh extremist leader's conversations, investigative personnel considered that there was no significant tape content and therefore they were not required to make any decision or to provide any direction on the retention or erasure of the reviewed tapes. Consequently, the disposition of these audiotapes was not subject to any formal and attributable erase/do not erase decision process but was an automatic erasure procedure left to those persons lowest in the responsibility hierarchy.

A brief review of one other similar case in the year following the disaster suggests that several of the problems we noted above were not unique to this investigation.

(h) Foreign Government Involvement

Allegations of wrong-doing in Canada by the Indian government, which long concerned the Sikh community, reached new heights in the wake of the Air India crash. Statements by leaders of the Sikh community and media articles produced a storm of controversy. The publication of the book, ``Soft Target'' in 1989 synthesized the allegations and accused the Government of India (GOI) in general and its foreign intelligence agency, the Research and Analysis Wing (RAW) in particular, of complicity in the crash. The conspiracy theories became widely known and still endure years after the tragedy.

We reviewed these allegations and others pertaining to any foreign government involvement in the crash. For each allegation, however, we either learned of credible explanations for the activity or, more often, the information we saw did not constitute trustworthy evidence in support of a conspiracy theory. That said, on one issue that we examined, the Service did not pursue its investigation in the years after the crash to the extent that we would have expected. The information that the Service did collect in this case was passed to the RCMP to review in the context of their criminal investigation.

The RCMP, which is conducting the criminal investigation of the Air India crash, has twice responded to questions about the involvement of the GOI. In November 1985, the RCMP publicly stated that such allegations were ``without substance or foundation''. In a briefing the RCMP provided to us in February 1992, the Force again stated that it does not have evidence to support this theory.

(i) Conclusions

On the basis of our findings, we conclude that prior to the disaster, CSIS was investigating potential threats posed by Sikh extremists in accordance with its mandate and in a manner consistent with the then perceived level of threat. We further believe that CSIS fulfilled its mandate to investigate the possible terrorist threats and that it advised the appropriate government and law enforcement agencies of the information it had in a timely and comprehensive way.

Based on our review of the information that CSIS possessed prior to the crash, the Service was not in a position to predict that the Air India flight was to be the target of a terrorist bomb.

In the absence of clear Service-wide policies to deal with a terrorist incident of this magnitude, we conclude that CSIS senior management did not provide the direction we would have expected concerning the Service's mandate and role in relation to the RCMP criminal investigation.

We also conclude that in the period following the disaster, all information in CSIS' possession that was relevant to the investigation was provided to the RCMP. Delays caused by incomplete or inadequate policies, however, did occur.

Disputes and difficulties over cooperation and the conduct of the investigation occurred between members of CSIS and the RCMP but these tended to be isolated and on a personal level, and we believe that they had no serious detrimental effect on the respective investigations.

We noted that the CSIS policies in relation to the collection, retention and erasure of surveillance audiotapes were seriously deficient as well as being generally inaccessible to investigators and that the informal procedures developed to compensate for these problems were also inadequate. Nevertheless, it is unlikely that the prevailing practices resulted in the loss of important information relevant to the disaster and the subsequent investigation.

We reviewed the CSIS information to assess whether an agency or representative of a foreign government was involved in the destruction of the aircraft. Based on the material we examined, the information collected by CSIS does not support the theory of complicity by a foreign government in the crash of Air India flight 182.

3. Case Studies

Attack on the Iranian Embassy in Ottawa

(a) Introduction

At about 12:18 p.m. on April 5, 1992, some 40 individuals armed with crowbars, sledge-hammers and a ladder attacked the Iranian embassy in Ottawa. Most were members of the Mujahedin-E-Khalq (MEK) and were protesting an Iranian air attack on the MEK base inside Iraq earlier that day.

The Ottawa attack began three hours after an attack on the Iranian embassy in Bonn, Germany. It was also preceded by at least seven other attacks in Europe.

Under the *Vienna Convention on Diplomatic Relations*, the host nation must protect embassies and diplomats. In Canada, their protection is the specific responsibility of the RCMP, with advice from External Affairs. CSIS has no protective functions, and its officials have no peace officer powers. Specifically, they are not authorized to carry weapons.

CSIS does perform some functions concerning embassies. For example, it provides intelligence concerning threats by issuing periodic threat assessments. It also advises the RCMP and local police of any specific threats against embassies that come to its attention. CSIS can, and often does, distribute relevant information from foreign intelligence services.

(b) Warning of the Embassy Attack

In March, 1991, CSIS provided an updated embassy ``threat assessment". It indicated an ongoing, moderate threat. The recent move of the Iranian embassy from a high-rise to a detached, four storey building may have made it more vulnerable to attack.

Reportedly, on September 19, 1991, someone threw a crude firebomb at the wall of the Iranian embassy. Damage was minor. There was no link between the firebomb and the April 1992 attack. Following the firebomb incident, the RCMP offered additional protection, which was refused.

Before April 5, 1992, no allied intelligence service, including CSIS, had predicted or forewarned of a possible imminent attack against Iranian diplomatic establishments. Indeed, there were signs of lessening tensions. The trend, despite a number of incidents, was away from violent attacks.

(c) The Day of the Attack

CSIS maintains a Crisis Management Centre (CMC) at Headquarters. The Duty Officer in the Centre monitors commercial wire services and radio and television news broadcasts around the clock. The Duty Officer has a range of tasks and follows a standard routine in reading reports from the printers and performing other duties.

Beginning at 7:12 a.m. on April 5, the CMC received a series of wire service stories about the bombing of the MEK base in Iraq. Some discussed the reaction of the MEK, but none referred to possible attacks on Iranian interests. Starting at 11:21 a.m., the CMC received three stories of disturbances in Europe.

Table 1. Information Received by Headquarters Crisis Management Centre

Wire Service Reports	Time stamp on report*	Cleared by Duty Officer
Bombing of MEK base in Iran (first of several)	7:12 a.m.	7:30 a.m.
Attack on Iranian embassy in Paris	11:21 a.m.	11:30 a.m.
Attack on Iranian embassy in Bonn	12:02 p.m.	12:15 p.m.
Attack on embassy at TheHague	12:05 p.m.	12:15 p.m.

* All times are Ottawa times.

No specific warnings came from allied intelligence services. The intelligence services and the media, it appears, thought the disturbances to be police matters and of strictly local interest. CNN, the news network, did not cover the story until approximately 4:30 p.m. Ottawa time — four hours after the attack on the Ottawa embassy. No specific warnings came from or through CSIS Security Liaison Officers (SLOs) in Europe. This is understandable, because there are few SLOs, and they have no specific responsibility for ``real-time" monitoring of the media.

CSIS did receive information that the Iranian air attack was in fact significant and might cause problems. However, no specific problems were identified. This information did not reach CSIS Headquarters before the embassy attack because it was given, in error, to the Ottawa Regional Office. That office did not learn of events in Europe until after the Ottawa attack because wire service reports are not usually received at CSIS Regional Offices. Headquarters had the wire

service reports about European events, and the Regional Office had information about possible problems, but neither had the complete story.

(d) CSIS Presence near the Embassy on the Day of the Attack

According to RCMP records, an RCMP vehicle conducted a routine check on the embassy at 12:12 p.m. The officer saw nothing unusual. When the attack occurred, CSIS was in the vicinity of the embassy for other reasons.

The attack on the embassy began at about 12:18 p.m.. Ottawa City Police received the first call about the attack from a private citizen at 12:19:31. Slightly later,
[1] CSIS Ottawa Region received a call from a CSIS employee, and the supervisor tried to telephone the RCMP. The telephone failed, causing a delay of about 30 seconds before another telephone was used. The RCMP received the CSIS call at precisely 12:21 p.m.

Press reports indicated that CSIS employees videotaped the attack. This is correct. CSIS personnel in the area of the embassy had been practising using a video recorder
before the attack. The camera was subsequently turned on to events at the embassy. The videotape begins with the words, ``call the RCMP", followed by ``Roger, Roger, I'm on the phone", the words of the Supervisor in Ottawa Region. Clearly, CSIS called the police before starting to record.

(e) CSIS-RCMP Cooperation

Claims have been made about allegedly poor cooperation between CSIS and the RCMP during the embassy attack. We asked the RCMP, Ottawa City Police and a host of individuals in the Service if there were such problems. Not a single person could cite any problem either in general or relating specifically to the embassy attack. A copy of the CSIS videotape was delivered to the RCMP within three hours of the attack for use in criminal investigations.

(f) Conclusion

The Service provided the Canadian government and the RCMP with an assessment indicating an ongoing, moderate threat. However, neither CSIS nor any other western police or intelligence agency had any specific warnings of attacks on Iranian embassies. There is ultimately no evidence pointing to a planned attack in Canada.

[1] We attributed the delay to the position of the CSIS personnel, who could not see the first activities of the attack.

On the day of the attack, CSIS activities were hampered because a telephone call meant for CSIS Headquarters was mistakenly rerouted to Ottawa Region. No one at Ottawa Region was aware of the error. Headquarters was thus denied significant information. The way CSIS handled information before the attack, therefore, was flawed. Intelligence was not collected and assessed at one location. The analysts at Headquarters, who are the ultimate experts, were not informed until after the attack. Still, would this information, if examined as a whole by the experts at Headquarters, have led a reasonable person to issue a warning to the police? We suspect not.

CSIS was in the vicinity of the Iranian embassy for other reasons when the attack began. Its presence was not in anticipation of the attack. A video recording was made. However, CSIS first called the police before starting the recording.

The ``Illegal''

In 1988, the Service began a two-year investigation after a suspected foreign intelligence officer and an individual from a developing country were observed meeting. The Service used surveillance, inquiries with allied intelligence services, interviews and other investigative tools.

It appeared that the intelligence officer was actively recruiting the individual, who showed signs of accepting. He obtained unclassified materials for the intelligence officer, agreed to covert meets and other security arrangements, and accepted small amounts of money. It seemed that his recruitment was nearly complete and that the intelligence officer was preparing him for ``bigger and better'' things.

The Service investigated vigorously. Through searches of records, CSIS identified the individual. CSIS officers had initially thought that he might have a false identity and might therefore be an ``illegal''.[2] CSIS carefully monitored his movements and meetings with the intelligence officer. The intelligence officer later left Canada. Overall, CSIS effectively defused a potentially dangerous spy operation.

The individual may have eventually represented a serious threat to the security of Canada. He was at one time accorded the highest level of targeting authorization — level 3 — which permits the use of all investigative powers. CSIS subjected him to fairly extensive investigation. This was appropriate in this case.

[2] An ``illegal'' enters a foreign country using stolen or forged documents. Once there, the illegal generally uses a different identity and nationality supported by a second or third set of documents. Illegals eventually try to acquire genuine documentation from the host country that supports their assumed identity. R.W. Corson and R.T. Crowley, *The New KGB* (New York: William & Morrow Company Inc., 1985) at 66.

The conduct of the investigation, however, involved discreet inquiries through a third party to a nation that has a history of human rights violations. Ministerial direction requires caution in any dealings with officials of such states. Given the parties involved and the Ministerial caution, our report suggested that there should have been consultation with the Minister.

There is no record on file to indicate that proper procedures were followed in obtaining some specific sensitive personal information. Furthermore, CSIS gave information identifying the individual to External Affairs. Section 19 of the *CSIS Act* requires a justification for such disclosures. In this case there was none, because CSIS had already defused the threat before the disclosure.

The investigation was pursued with appropriate tenacity and zeal. Later findings were to confirm that the investigators' instincts in this case were correct.

4. Activities During the Gulf Conflict — Community Interviews

In 1991-92, the Committee analyzed in depth the CSIS community interviews program that operated during the Gulf conflict. Our study sought to respond to the concerns expressed by the Canadian Arab Federation (CAF) in its special executive report: *The Canadian Security Intelligence Service (CSIS) and the Arab Canadian Community*. We were also responding to concerns that the British Columbia Civil Liberties Association (BCCLA) raised in a section 41 complaint to the Committee.

Specifically, we attempted to determine whether:

- the interviews program complied with legislation, Ministerial direction and CSIS policy and procedures;
- the interviews program was ``strictly necessary'' to advise the Government of Canada about threats to national security;
- the information collected from the interviews and retained on files was relevant to the activities being investigated; and
- the way CSIS investigators conducted the interviews was unnecessarily intimidating, coercive, or public.

Our investigators identified community interview reports in CSIS files. We examined CSIS Headquarters instructions to regions about interviews. We interviewed CSIS managers. We met with ten Arab Canadians who had been interviewed by CSIS. We told them that they would not be subject to retaliation in any event, but also assured them that their names would not be provided to CSIS or to any other department.

Specific Findings

We may never know the exact number of individuals contacted by CSIS during the Gulf conflict. This is because no specific code was used for the entry of the interview reports in the CSIS database. However, we are satisfied that there were about 187 interview reports. There may be more contacts that were not reported by CSIS investigators.

The Canadian Arab Federation Concerns: The CAF report expressed numerous concerns. We attempted to answer the following specific CAF allegations:

1. That CSIS exchanged information with foreign agencies, specifically with the Israeli Secret Intelligence Service (Mossad).[3]

[3] CAF Executive Report, page 2.

Our finding: We could not find any evidence that CSIS communicated any information or intelligence generated by the community interviews to any foreign agency.

2. ``CSIS activities were intended, at least in part, to have a chilling effect on the Arab Canadian community."[4]

Our finding: We found no evidence that the Service actually intended to have a chilling effect on the community. Due to the stress caused by this intense international crisis, the uncertain immigration status of some persons interviewed and the poor reputation of security services in the Middle East, it is quite likely that some interviews did have a chilling effect.

3. The interviews with Arab Canadians were inherently abusive in that the primary criterion in selecting the individuals was their Arab origin. CSIS' administration of a loyalty test through the question ``What do you think of the war in the Gulf?" was insulting and demeaning to Arab Canadians.

Our finding: It was not ``inherently abusive" to meet members of these communities to determine whether threats to the security of Canada might emanate from the Gulf crisis. Nor can it be inferred that CSIS was questioning the loyalty of Arab Canadians simply by seeking the views and intentions of some elements of the community.

4. ``A large portion of the Arab Canadian community has a very different experience with secret police forces in other parts of the world. Indeed, the psychological impact of a CSIS visit, especially when done without prior notification, was often massive. The line of questions CSIS officers asked Arab community members was often irrelevant and demeaning. Specifically, some questions related to religious beliefs, and technical information, such as that regarding citizenship."

Our finding: We believe the fears expressed by some individuals contacted by CSIS and found them understandable. It is worth noting that there have been two other community interviews programs since the Gulf crisis, and that there have not been any complaints arising from either of them.

The Canadian Arab Federation Case Studies: The CAF report described five cases where CSIS had allegedly acted improperly. We met the three individuals mentioned in three case studies. For the other two cases, we sent formal questions to CSIS and reviewed files.

[4] CAF Executive Report, page 8.

1. Arab Canadians placed under surveillance: The CAF alleged that some Arab Canadians were placed under special surveillance. For example, it was alleged that CSIS paid a surprise visit to a man's home and asked questions about his religion, attendance at a mosque, and the political affiliations of his family members.

Our Finding: This case illustrates the difficulty we faced because of the generality of some allegations. A member of the Committee met with the individual concerned. The individual expressed concerns about the surprise nature of the visit, the fact that he was being consulted not as a Canadian citizen, but rather as an Iraqi, that simplistic conclusions would be reached from his answers on his religious beliefs, and that answering questions about his family's political affiliations could prevent them from being accepted as landed immigrants. We recognize that a knock on the door or a telephone call by a representative of a secret service can be quite a surprise for ordinary citizens. However, we believe that, when conducted properly, a direct approach is the best procedure for a community interviews program. We also found that the Service did not reach simplistic conclusions on the individual's religious beliefs, and that no exchanges of information with the Department of Employment and Immigration or other domestic agencies occurred in this case.

2. CSIS surveillance in violation of its mandate: Last year we reported on allegations that CSIS had conducted inquiries or interviews at the University of Calgary.

Our Finding: We examined the allegations further and confirmed that the Service had conducted no inquiries or interviews there.

3. Enticement — CSIS offer of protection for information: The CAF report alleged that CSIS offered protection to a man in return for information about the Iraqi community. He apparently refused.

Our Finding: Our staff met the man and found that the offer for protection was more evident to the CAF than to the individual. There was no evidence of direct enticement.

4. CSIS photography of Arab Canadians: The CAF alleged that an Arab Canadian was shown several photographs of ordinary Canadian citizens of Iraqi origin.

Our Finding: We questioned the Service about the photographs. The Service replied that, with one exception, all the photographs were of foreign nationals with no status in Canada. We have learned that the exception fell within the mandate of the Service.

The CAF also claimed that the Service had met three times with the individual. CSIS allegedly visited him at his apartment and took him to a meeting which lasted more than five hours in a six-by-ten foot room with no windows or clock.

Our Finding: We reviewed the accounts of those interviews. According to CSIS, this individual had been met only twice, both times at CSIS offices. We also met the individual. He stated that he met only twice with CSIS. Both meetings were held at CSIS offices.

5. CSIS monitoring of Arab Canadian telephone traffic and visit by CSIS: We asked the Service to produce all the information it held about one individual. We reviewed all relevant CSIS documentation. We also contacted the individual.

Our Finding: We found nothing to confirm the tapping of the phone line or the CSIS visit. We confirmed that CSIS did nothing inappropriate or illegal.

The British Columbia Civil Liberties Association Concerns: In a letter dated April 15, 1991, the BCCLA complained to the Director of CSIS about CSIS interviews of Arab Canadian community members. The Association had received reports from the Canadian Arab Federation that visits by CSIS agents were unannounced and had been informed that interviews were sometimes unnecessarily public and coercive. The BCCLA was also informed that several interviews involved inappropriate questions.

On May 27, 1991, the Director wrote to the President of the BCCLA saying that the Service had met with fewer than 200 individuals across Canada. CSIS believed that these individuals could help CSIS. The Director said he was always concerned by allegations that CSIS employees may have acted illegally or inappropriately. The Director's letter continued that, short of seeing the details of a specific case, he could say with confidence that ``CSIS employees acted responsibly, within the law and policy and in accordance with the expectations of Canadians that the Service would be on guard in the face of the very explicit threats of terrorism that had been made".

The BCCLA was not satisfied with this response. On June 20, 1991, the BCCLA President submitted a formal complaint to us. Our Executive Director and Senior Complaints Officer met the President and the Vice-President of the BCCLA to discuss their concerns. Because there was no specific complaint by Arab Canadians, it was agreed that a general review of CSIS activities would be the best approach for the Committee to take.

The BCCLA request covered three topics. The requests, and our responses, follow:

(a) SIRC should review the reports of CSIS officers who visited citizens and residents of Arab and Iraqi descent during late 1990 and early 1991 to determine, if possible, whether the visits were unnecessarily coercive or public.

Our response: It was difficult to establish precisely whether the approaches were in fact coercive. However, the visits were sometimes perceived as coercive. This is primarily because the persons interviewed were rarely told that the interview wasoptional. We know of only four cases where CSIS made it clear that the interview was optional. In some other cases, the

individuals were clearly reluctant to meet, but eventually agreed. In a few instances, the Service sought information about Arab Canadians from other people or organizations.

(b) SIRC should seek out the views of members of these ethnic communities on the nature and result of the visits to their members by CSIS officers.

Our response: The CAF report states that ``to the frustration of the Canadian Arab Federation, Arab Canadians who reported their cases to it are concerned about retaliation and now prefer to forget the incidents rather than file official complaints . . .". We have experienced the same frustration. We depended on the President of the CAF to facilitate access to the community. Finally, we met with ten persons. We exhorted them to encourage others to meet with us, but to no avail.

(c) If SIRC determines that the scope of the visits or the manner of the approach was inappropriate, given the sensitivities of members of these communities, SIRC should make a report to the Solicitor General of Canada containing its findings, and provide recommendations to CSIS for addressing any areas of concern.

Our response: We found that the community interviews program was appropriate and strictly necessary to advise the government about threats to national security.

General Conclusions and Recommendations

Compliance with legislation, Ministerial direction, and CSIS policy and procedures: The interviews program complied with the law. It was a duly authorized investigative activity.

The community interviews program is designed to evaluate the presence and magnitude of a suspected threat to the security of Canada. CSIS is not, therefore, investigating the individuals it wishes to interview. It need only establish their identity. However, because the community interviews program requires a TARC level 2 authorization to proceed, CSIS investigators have more authority than is necessary to conduct a simple identity check.

Recommendation:

The Committee recommends that, in the normal course of events, a community interviews program be authorized at a special TARC level 1, with full authority to collect any information strictly necessary to establish the identity of prospective interviewees. This special level 1 authorization would require the approval of the Director or Deputy Director Operations at CSIS Headquarters.

Retention of Information about Persons Interviewed: Even a program to obtain strictly limited information about a prospective interviewee can result in a considerable amount of information accumulating in CSIS files. Since the individuals concerned are being asked to assist CSIS in identifying a possible threat to the security of Canada and are not targets themselves, it would be wrong for more than a minimum amount of personal information about them to be kept in CSIS files.

Recommendation:

The Committee recommends that within a reasonable period following the completion of a community interviews program, the information held by CSIS on individuals interviewed be reduced to the absolute minimum required to record the person's identity and the fact that an interview was conducted.

Was the Community Interviews Program Necessary?: During the Gulf conflict, various regimes called for terrorist actions against Iraq's opponents. Canada was among those opponents and was not immune to acts of terrorism. It was the responsibility of CSIS to enhance its understanding of the environment from which threats might arise. The interviews program was strictly necessary to advise the Government of Canada about threats to national security.

Relevance of the information to the activities being investigated: There is often a strong sociological relationship between the state and religion in Middle Eastern countries. We believe the Service would have been negligent if it had not taken this into account during the community interviews program.

The way CSIS conducted interviews: We recognize the danger in making a global assessment. It might not sufficiently reflect specific circumstances and events that came into play in individual interviews. With this caveat in mind, we conclude that CSIS conducted the interviews in a professional manner. The ten individuals we met stated as much. We have found nothing to confirm the allegations of harassment. If there was any ``sense of intimidation" arising from the interviews as described by the CAF (and we are not disputing that some of the other 177 individuals approached by CSIS may have felt intimidated), we believe it may well have been due to the intense international crisis, the uncertain immigration status of certain persons interviewed, and the reputations of security services in certain areas of the world for unscrupulous conduct.

We did find that, in a few cases, the way CSIS approached individuals was quite forceful. For example, some individuals resisted the proposal for an interview when CSIS telephoned them, but CSIS later interviewed them nonetheless.

5. Other CSIS Operations

Arrangements with Other Governments

(a) Foreign Arrangements

In 1991-92, the Service received Ministerial approval for the establishment of four new or expanded foreign arrangements. Two involved countries with poor human rights records. Of these, one is contingent on the foreign agency meeting certain conditions which, to date, have not been fulfilled.

(b) Domestic Arrangements

During the same period, the Service concluded one permanent Memorandum of Understanding (MOU). The MOU, signed with Quebec's Department of Public Safety, covers exchanges of information between CSIS and the *Sûreté du Québec*, the Montreal Urban Community Police Force and other municipal police forces.

Exchanges of Information with Foreign and Domestic Agencies

(a) With Foreign Agencies — London and Paris

Subparagraph 38(a)(iii) of the *CSIS Act* requires the Committee to review arrangements entered into by CSIS under subsections 13(2) and (3) and 17(1) of the Act. These include arrangements with foreign states. The Act also authorizes us to monitor the information and intelligence provided under the arrangements.

Under this authority, we conduct a review every two years of a sample of the correspondence from CSIS to foreign agencies. We do this to ensure that CSIS has made no excessive or unnecessary use of its powers. Our most recent review also examined key issues pertaining to the operations at the foreign posts and the organization of the Field and Liaison Unit at CSIS Headquarters.

In the summer and fall of 1991, we reviewed what information and intelligence CSIS had released to British and French agencies, then assessed whether the releases complied with the *CSIS Act*, Ministerial direction and CSIS policies and procedures. We conducted our reviews at CSIS Headquarters in Canada and at the Security Liaison Officer posts in London and Paris.

The first samples of material from the two posts were exchanged during the Gulf War — a critical period for the Service and its counterparts abroad.

The Committee looked at several issues: the statutory basis for the retention, dissemination or receipt of the information; compliance with foreign arrangements; accuracy of the information provided by CSIS; whether the importance of the investigation outweighed the potential damage

to individual rights resulting from disclosure of information; and the controls in place at Headquarters and at posts abroad for the material the Service releases.

Findings: Our review concluded that releases of information by the two posts examined have been appropriate. Correspondence exchanges complied with the foreign arrangements and met the statutory requirements for the retention, dissemination, and receipt of information. Our criticisms focused almost entirely on the absence of or deficiencies in policy.

In our 1989-90 Annual Report we discussed the information exchanged with agencies under foreign arrangements (Chapter 5). We noted that the former Foreign Liaison Branch served an important control function as the main liaison between Headquarters and Security Liaison Officers abroad. The Branch no longer exists. Many of its roles have been reassigned to Foreign Liaison Advisers attached to the Counter-Terrorism and Counter-Intelligence Branches.

With the operational branches bearing these new SLO responsibilities, one might have expected that CSIS would have developed policy to assist them. Instead, we found major gaps in general written policies governing SLOs and the management of information sent to countries or agencies with poor human rights records. Despite this problem, the exchanges with Britain and France we examined were handled responsibly.

We concluded that SLOs at the posts should be more proactive in information exchanges. As well, we concluded that CSIS Headquarters should use the French language in messages to France. On the positive side, we noted that CSIS received compliments from some allied agencies for its threat assessments and its reports from the Analysis and Production Branch.

(b) With Domestic Agencies

Under subparagraph 38(a)(iii) of the *CSIS Act*, the Committee is to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(1). These include arrangements to provide security assessments or other cooperation to provincial governments and provincial police forces. The Committee is to monitor the provision of information and intelligence under these arrangements.

In September 1990, the Committee provided to the Minister a special report under section 54, entitled ``Domestic Exchanges of Information". The report made several recommendations. One called for establishing a uniform, national tracking system for domestic exchanges. In the spring of 1991, CSIS set up the new tracking system in each region and at CSIS Headquarters. This year, the Committee completed a review of the new system and performed an audit of exchanges tracked under it. We examined actual operations and other files in two regions.

The new system is simple. Operators place the code of the donor of the information (the organization providing the information) and the recipient (the one accepting the information) on the forms containing the information. These forms can then be retrieved by computer. No actual list of exchanges is retained.

The system seems to work well. Users are having little difficulty with it. Coding errors sometimes occur, but they are neither common nor serious. Staff have been adequately trained to use the new system.

The system, however, suffers from a lack of definitions in crucial areas. What sorts of information constitute an exchange that must be logged — information passed orally, information obtained directly from files, written exchanges made in the absence of section 17 agreements? The instructions to users provide no answers. Differences in interpretation have resulted in a considerable variation in the application of the logging system between regions.

As part of the review, we examined the operation of section 17 agreements. In general, the agreements have been functioning well, though there have been some minor problems. In particular, we examined exchanges of information between CSIS and the RCMP. Recently, CSIS has allowed the RCMP greater access to raw investigative materials.

We reviewed exchanges with other police agencies. Co-operation appears very good, though we found a complaint by one police agency that information was being withheld. We also noted possible procedural impediments within CSIS to the sharing of ``perishable" information — information that is valuable now, but that will be of no use within a short time.

We also examined the use by CSIS of ``sensitive" information. By sensitive, we mean medical, welfare and other similar information. CSIS officers we spoke to in two regions appeared very careful to avoid using sensitive information, and indicated that they rarely saw an operational reason for its use. Of the approximately 4,000 documents we examined, we found only one to be somewhat sensitive. This item had been used to positively identify an individual.

As part of the general audit, we assessed whether exchanges comply with the *CSIS Act*, other statutes, and the agreements with other agencies. We also examined whether the intrusions into personal privacy caused by exchanges were proportionate to the potential threat.

We concluded that the vast majority of the exchanges were properly handled. However, a few concerns surfaced. Sometimes the Service obtained access to information in files on individuals held by federal departments. Except for purposes related to security screening, such access should be reserved for the more intrusive investigations, and generally the Service should obtain only

specific information from such files. We have recommended that CSIS develop specific policies about full access to government files and that any request for full access be logged as an exchange.

As we reported last year, CSIS provides and obtains information concerning public demonstrations. Usually, this information concerns embassies, VIPs or potential serious violence. We found no problems with this process. However, the rules in the CSIS Operational Manual governing reporting on demonstrations are antiquated and make no reference to the *CSIS Act*. We have recommended that they be amended.

Warrant Statistics

Under the *CSIS Act*, the Service must acquire warrants from the Federal Court of Canada to use telephone intercepts and other intrusive investigative tools and devices. We publish statistics provided by CSIS on warrants issued. The Service reported as follows:

Table 2. New and Renewed Warrants, 1989-90 to 1991-92

	1989-90	1990-91	1991-92
New warrants granted	34	27	39
Warrants renewed	50	51	73
Total	84	78	112

There has been a significant increase in the number of warrants since last year. However, there has been only a slight increase in the number of targets subject to investigations authorized by warrants.

Last year, the Committee for the first time provided a general indication of the number of persons subject to investigations authorized by warrants. There has been very little change since then. Canadians and landed immigrants directly affected by CSIS investigations under Federal Court warrants still number in the hundreds, not in the thousands.

Last year, the Committee began compiling its own statistics on warrant use, instead of relying on statistics provided by CSIS. We can now better assess the frequency of use of investigative techniques authorized by warrants, and can ask CSIS more informed questions.

Warrant Product: In Chapter 2 of this report, we discuss backlogs of audiotapes which contained intercepted communications. Since 1985, much has changed at CSIS in the handling and processing of this type of warrant product. New policies have been developed and employees have been informed about the changes. The new controls and tracking system provide

accountability.

The Committee was told that in the first half of 1992, there were cases where backlogs of tapes existed. In two-thirds of these cases, CSIS has given a satisfactory reason for the backlogs and the measures taken to eliminate them. We are, however, concerned about a significant backlog in one region and we are pursuing the matter.

Counter-Terrorism (CT) Program

Counter-Terrorism Branch: The past year in the Counter-Terrorism Branch might best be described as ``business as usual''. Still, this means that a great deal of activity indeed took place in the Branch. At the beginning of the fiscal year, the Service was completing its investigative activities relating to the Gulf War. We reviewed those activities in Chapter 4. Shortly after the fiscal year ended, the Iranian embassy in Ottawa was attacked. We reviewed this incident in Chapter 3. Amidst these publicly known events, the covert work of the Branch continued apace.

The Branch has recognized that the dynamics of international terrorism will change in response to the new international alliances, such as those formed during the Gulf crisis. As a coalition partner during the ensuing war, Canada may have become a more desirable terrorist target. Resource allocations within the Branch have changed accordingly. Situations are also changing on the domestic front, and the Branch strives to anticipate and respond to the resulting terrorist threats. The recommendations of the Director's task force now assessing the operational priorities of the Service (see Chapter 9) may profoundly affect the direction of the Branch in the 1992-93 fiscal year.

We are interested in how the Branch responds to changes in Canada as well as changes abroad. We will be especially vigilant about CSIS actions which might have an impact, no matter how inadvertent, on the domestic political process.

Threat Assessments: CSIS issues threat assessments to its clients in other federal departments and agencies. During the 1991-92 fiscal year, the Threat Assessment Unit produced 885 threat assessments. This represents a substantial decrease from the previous year's total of 1,145. The 1990-91 total was higher due to the Gulf hostilities and several other investigations then ongoing.

Research Studies: In our 1988-89 Annual Report we repeated our concern that the research function in the Counter-Terrorism Branch was suffering because the unit responsible for research was also responsible for briefings. Demands for briefings were frequent and urgent, and often displaced the research function. We still maintain that the Branch would benefit from having a separate research unit to consolidate operational intelligence. This would enable the Branch to determine patterns in global trends, thus allowing the Branch to better determine new threats. The supremacy of the briefings function is shown by the recent name change to the ``Briefing and

Production Unit". CSIS notes that the research and analysis of the Analysis and Production Branch (RAP) is carried out in close conjunction with the CT Branch.

During 1991-92 the Branch prepared a study of the incidents and threats of terrorism in Canada from 1988 through 1991. The summary also contained a trend analysis and a synopsis of significant cases where the efforts of CSIS prevented terrorist acts. We have asked for a copy of the study.

Post-Mortem on Open Skies Conference: In 1991-92, the Committee received a post-mortem report from the Service on its activities during the Open Skies Conference held in Ottawa in February 1990. The most important function of CSIS during special events is to disseminate timely threat assessments and to respond quickly to any incidents. No incidents occurred during the event.

The post-mortem report addressed key issues relevant to CSIS managers. The Committee learned from the report that CSIS internal communications were not trouble-free. The recommendations contained in the final version of the post-mortem report may solve these problems. We will reassess this issue next year.

Counter-Intelligence (CI) Program

The extraordinary changes in the old Soviet Union and collapse of the Warsaw Pact have radically altered the *raison d'être* of the Counter-Intelligence Branch. Not only the targets themselves, but the fundamental basis for investigating the activities of officials from these countries have come into question.

The Counter-Intelligence Branch has a particular interest in the outcome of the CSIS task force review. To date, we have seen some shifting of resources from Counter-Intelligence to Counter-Terrorism. We have also seen the rise of a new entity, ``Requirements — Technology Transfer''. The Technology Transfer Unit has operational and analytical components at Headquarters, as well as coordinators in all regional offices. The Unit investigates technology transfer issues, specifically the increase in destabilizing technologies and the foreign transfer of technology detrimental to Canada's economic security.

The Director's task force report (see Chapter 9) will have a direct impact on the Technology Transfer Unit. After it reviews the report, the Committee will closely examine the mandate and functions of the Unit

Analysis and Production Branch (RAP)

In February 1992, the Service reorganized the structure of RAP; it changed from having three geographical sections to two. A new functional unit devoted to strategic and issues-oriented analysis was also established. The new unit will address emerging security intelligence issues that are not focused geographically. The Service claims that a need exists for more intelligence on technology transfers, economic espionage, financial movements and significant environmental, health and refugee crises which could constitute threats to Canadian security.

A fourth section deals with administration and support issues. One objective of the reorganization is to develop and manage a CSIS marketing and client liaison program. The program would help CSIS produce more relevant products through closer collaboration with clients.

Once again this year, RAP increased its overall intelligence production. The Branch increased the quantity of intelligence reports on threats emanating from terrorism. At the same time, reports dealing with counter-intelligence matters were fewer, a result of the political developments in Eastern Europe. We noted with pleasure the hiring of a full-time French editor.

(a) ***Commentary***

The Analysis and Production Branch published 12 issues of *Commentary* during the fiscal year. This unclassified publication addresses broad concepts and strategic situations. The topics covered are:

1. Post War Iraq, Gulf Security and a ``New World Order''
2. Can de Klerk Control the Violence in South Africa?
3. Problems of Postwar Gulf Security
4. Where is the Soviet Union Heading?
5. Prospects for the Middle East Peace Process
6. Terrorism and the Rule of Law: Dangerous Compromise in Colombia
7. The Soviet Disunion
8. De Klerk's Relationship with the South African Intelligence Services
9. Yugoslavia: Nations, Nationalities and Other Nationalities
10. Three trips: Terrorism: Forecast for the 1990s; International Security: Who's on First?; The Abortive Hijacking of Alitalia Flight #864
11. Azerbaijan and Armenia: Land or Peace?
12. Intelligence Needs of Newly Industrializing Countries in the 1990s.

(b) Science and Technology

As required by a Ministerial direction, the Branch prepared a series of studies on the threat to various high-technology sectors in Canada. The Service justified these studies as follows:

> Recent technological developments, business ``globalization'', the end of the Cold War, and the continuing revolutions in Eastern Europe and the Soviet Union, all indicate that economics will play an increasingly important role in international affairs. Just as military security was considered to be heavily dependant on defence-related research and development (R&D), so also is a country's economic security (i.e. its competitiveness and standard of living) now considered to be largely dependant on the research, development and adaptation to new technologies.
>
> This link between technology and economic competitiveness has resulted in a re-examination of the concept of national security, with national security being increasingly defined in economic terms. This has led to the recognition that, in the future, a country's political and military allies may well be, at one and the same time, its greatest economic competitors.
>
> There is a concern therefore, that Canada and Canadian companies not be placed at a disadvantage or exposed to possible damage as a result of state-sponsored economic espionage. Whether an espionage case is of an economic or military nature, the result could be that public or private funds are wasted or their full benefits not realised, resulting in damage to Canada's national interests. **Source: CSIS Study 91/58**

(c) Executive Intelligence Production Committee

The Executive Intelligence Production Committee (Executive IPC) is responsible for providing overall direction to RAP. In 1991-92, the Executive IPC met three times.

Files

(a) File Management

In fiscal year 1991-92, CSIS reviewed 230,400 files, destroyed approximately 190,000 of them and sent 1,822 of historical value to the National Archives. The rest have been reclassified into other file categories. Access to most of these files is restricted. Special procedures are in place to ensure that senior management approval is obtained before Intelligence Officers are permitted to review the restricted material.

We noted that CSIS reduced drastically the number of files on Canadian ``right-'' and ``left-wing'' subversives.

In 1991-92, CSIS opened approximately 80,000 files. The vast majority were screening files (immigration, citizenship, government security checks, and checks for foreign agencies).

(b) The Special Case of Files Inherited from the RCMP Security Service

We have for several years followed the status of the 510,000 files inherited from the RCMP. Last year, we reported that CSIS had reviewed slightly more than half of them. In 1991-92, the Service reviewed a further 31,287 files. It retained only 1,214 of these. The rest (30,073) were either destroyed or transferred to the National Archives. Some 208,671 inherited files remain to be reviewed by CSIS.

In April 1992, the media issued several reports about security files on homosexuals. Homosexuals were supposedly investigated by the RCMP Security Service in the 1950s and 60s. We asked CSIS about the existence of these files. The Service told us that the RCMP destroyed the files in the early 1980s and that CSIS never received them.

Internal Security

In last year's annual report, we spoke of an internal security case involving the RCMP Security Service. We also indicated that we would examine CSIS internal security investigations further. This year, we completed our study of internal security. For security reasons, we cannot give details of our findings. However, we can say that there have been some weaknesses in the past, perhaps, in handling internal security matters. The Service has addressed these weaknesses. We can also say that the Service appears to be very vigilant against penetration attempts by foreign intelligence services.

Domestic Terrorism

Our 1990-91 Annual Report described our review of Service investigations of politically motivated terrorism in Canada. Section 12 of the *CSIS Act* authorizes CSIS to make such investigations. We examined how CSIS investigated threats from racist extremists and persons engaged in single issue political violence.

The Service should have reported to the Minister that one operation was likely to generate controversy. The Service consulted with External Affairs and had sought the Solicitor General's approval for the operation. However, it did not possess complete information when it told the Minister that it expected no problems from the operation. The Service should have been more

aware of the potential for controversy and the possibility of unlawful activity. Accordingly, we recommend that the Service take certain actions in such situations.

National security concerns prevent giving further details about this case. However, we will shortly issue a section 54 report to the Solicitor General describing our concerns in detail.

Section 16 Investigations

Section 38 of the *CSIS Act* requires the Committee to monitor requests by the Secretary of State for External Affairs or the Minister of National Defence for CSIS to conduct investigations under section 16 of the Act. Section 16 allows CSIS to collect information or intelligence about foreign states or persons in relation to the defence of Canada or the conduct of international affairs.

The Committee ensures that the appropriate Minister has requested the investigation and that the targeting complies strictly with section 16. The Committee also examines security intelligence ``spin-off'' provided to CSIS. We audit whether the information CSIS collects about Canadians, if any, is justifiable under section 12 of the *CSIS Act* and is retained in accordance with that section.

The Committee does not, however, review information provided to the Minister of National Defence or the Secretary of State for External Affairs as a result of a section 16 investigation. Our role is strictly limited to reviewing security intelligence ``spin-off'' and requests from Ministers. In the case of section 16, CSIS is merely providing a service for the collection activities of another department.

The Quebec Delegation in Paris

We were advised of a press report that CSIS had been spying on *La Délégation générale du Québec* à Paris. So far, we have seen no evidence of CSIS activity in this regard, based on our queries within Canada and our on-site review of the CSIS post in France (see Chapter 5). We will continue to monitor this matter.

6. Complaints

During the 1991-92 fiscal year, we received 30 new complaints, five fewer than the year before. Most were made under section 41 of the *CSIS Act*; they were complaints about ``any act or thing done by the Service".

Table 3. Complaints, April 1, 1991 to March 31, 1992

	New Complaints	Carried Over from 1990-91	Closed in 1991-92	Carried Over to 1992-93
Security Clearance	3	0	3	0
Citizenship	0	0	0	0
Immigration	0	0	0	0
Human Rights	0	0	0	0
Section 41	27*	4	28	3
Total	30	4	31	3

* Of the 27 complaints, 7 were outside the Committee's jurisdiction.

Of the remaining twenty, thirteen concerned individuals who believed that they were the subject of undue surveillance by the Service. We were able to satisfy these complaints. Three were advised to contact CSIS and were satisfied with the Director's response. The remaining four complaints were fully investigated by the Committee.

Mandate: Section 41 of the *CSIS Act* directs the Committee to investigate complaints made by ``any person" with respect to ``any act or thing done by the Service". Before the Committee investigates, however, two conditions must be met:

(a) The complainant must have first complained to the Director and not received a response within a period of time that the Committee considers reasonable or the complainant must be dissatisfied with the Director's response; and

(b) The Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Furthermore, under subsection 41(2) the Committee cannot investigate a complaint that can be channelled through another grievance procedure under the *CSIS Act* or the *Public Service Staff Relations Act*.

This year, many section 41 complaints involved persons who believed that they were being subjected to undue surveillance by CSIS. We chose to comply with the policy of the Service neither to confirm nor deny that a person is a target. However, we thoroughly investigated the allegations to ensure that:

(a) the Service has not used and is not using its powers unreasonably or unnecessarily; and

(b) the Service is performing its duties and functions effectively, efficiently and legally.

Some other section 41 complaints were made by employees of CSIS who had not yet used the internal grievance procedure. One complaint concerned a job applicant who had been refused a position by CSIS. Subsection 8(1) of the Act gives the Director the ``exclusive authority to appoint employees and, in relation to the personnel management of employees . . . to provide for the terms and conditions of their employment". Subsection 41(2) does not permit us to handle such complaints. We advised these complainants of the other recourses available to them.

One complaint involved a delay by CSIS in processing a person's application for permanent residence. In the midst of our investigation, CSIS issued its recommendation to the Canada Employment and Immigration Commission (CEIC) and the complainant decided not to pursue the matter.

Complaints about security clearances: Under section 42 of the Act, a complaint can be made to the Committee by:

(a) a person refused federal employment because a security clearance has been denied;

(b) a federal employee who is dismissed, demoted or transferred or denied a promotion or transfer for the same reason; and

(c) anyone refused a contract to supply goods and services to the government for the same reason.

The limitations of section 42: Section 42 clearly provides a recourse for public servants and those contracting directly with the government if they are denied a security clearance. However, persons employed by contracting companies, such as employees coming under the Airport Restricted Area Access Clearance Program (ARAACP) have no such right. Their only recourse lies in taking their case to the Federal Court.[5]

[5] In last year's annual report, we recommended that the government instruct all departments to treat any denial of a security clearance as if it were covered by section 42.

We declined to hear a case which dealt with correspondence from a representative of an employee under the Airport Program (ARAACP). We explained the inherent deficiency in section 42 and suggested that if the complaint was related to the length of time taken, type of questions, or both, the employee could complain to the Director of CSIS. The individual did not pursue the matter.

Citizenship, immigration and human rights complaints: As in the last three fiscal years, we received no complaints in 1991-92 about refusals of citizenship or rejections of persons as inadmissible under the *Immigration Act.* Similarly the Canadian Human Rights Commission has not referred any cases to us in the last three years.

Supreme Court of Canada Decision in *Chiarelli*[6]

The Federal Court of Appeal, in *Chiarelli v. Minister of Employment and Immigration*,[7] found that subsection 48(2) of the *CSIS Act* was so broadly worded that it contravened the *Canadian Charter of Rights and Freedoms*. That subsection states in part that ``no one is entitled as of right to be present during, to have access to or to comment on representations made to the Review Committee by any other person".

The Committee, however, has always interpreted subsection 48(2) very narrowly. We believed that this interpretation conformed with the letter and spirit of the Court of Appeal decision. Only evidence which, if made public, would harm Canada's national security, reveal the identity of a human source, or reveal the methods of operation of an investigative agency has been withheld from applicants or complainants. In such cases, the Committee's counsel has been instructed to compensate by vigorously cross-examining CSIS or other government witnesses. The Committee has also provided a summary of the main points of the evidence withheld to the complainant and counsel.

The Supreme Court of Canada heard a further appeal and rendered its judgment on March 26, 1992. The Court ruled that the *CSIS Act* and the Review Committee Rules recognized the competing individual and state interests and attempted to find a reasonable balance between them. The Court noted that the Rules expressly directed that the Committee's discretion be exercised with regard to this balancing of interests.

The Committee interprets this decision as recognizing that we conduct investigations and hearings fairly and responsibly.

---

[6] *Minister of Employment and Immigration* v. *Chiarelli and The Security Intelligence Review Committee* (26 March 1992), (Supreme Court of Canada) [unreported].

[7] *Chiarelli* v. *Minister of Employment and Immigration* (23 February 1990), (Federal Court of Canada).

Supreme Court of Canada Decision in *Thomson*

The Supreme Court of Canada judgment in *Thomson*, delivered on February 13, 1992, marks the end of a long battle by one of our first complainants. Mr. Thomson had been offered a senior position with Agriculture Canada in 1984, but the offer was rescinded after the Department's Deputy Minister denied him a security clearance based on the advice of CSIS. Mr. Thomson then filed a complaint with the Committee under section 42 of the *CSIS Act*. We issued a report under section 52 of the Act recommending that Mr. Thomson be granted the security clearance. The Deputy Minister decided to maintain his decision to deny the security clearance.

Mr. Thomson then asked the Federal Court of Appeal to set aside the Deputy Minister's decision. The Court ruled that a recommendation by the Committee was binding on the government official to whom the recommendation was made. However, the Appeal Court sent Mr. Thomson to the Trial Division of the Federal Court to obtain an order forcing the Deputy Minister to comply with the Committee's recommendation.

The judge in the Trial Division decided that he would not abide by the Court of Appeal's view that SIRC's recommendation was binding on a Deputy Minister. Therefore, he denied the application because he concluded that ``recommendations'', according to the ordinary meaning of the word, were simply the offering of advice.

Mr. Thomson then went before the Federal Court of Appeal a second time. The Court overturned the decision of the Trial Division, and ordered the Deputy Minister to grant Mr. Thomson a ``secret'' clearance.

The federal Crown appealed the decision to the Supreme Court of Canada. The issue, once again, was whether Deputy Ministers were bound to follow SIRC's ``recommendations''. The focus, therefore, was on the meaning of the word ``recommendation'' found in subsection 52(2) of the *CSIS Act*. In a 6-1 ruling, the Supreme Court held that ``recommendation'' should be given its ordinary meaning — the offering of advice — and should not be taken to mean a binding decision.

7. Security Screening

Sections 13, 14 and 15 of the *CSIS Act* provide the authority for CSIS to do security screening. The Service advises government departments on the following: government security screening, immigration and citizenship screening and refugee status determination. It also performs screening on behalf of foreign agencies.

Government Security Screening

In 1990-1991, the Service sought to reduce average processing times for security clearances to the following: 30 calendar days for Level I (Confidential), 30 days for Level II (Secret) and 120 days for Level III (Top Secret). As of December 31, 1991 the Service had surpassed its goals. Average processing times were 19 days for Level I, 19 days for Level II and 108 days for Level III.

This improved turnaround time has several causes, including a decrease in requests from departments and increased efficiency due to policy and procedural changes. For example, departments now submit criminal record check requests directly to the RCMP instead of using the Service as an intermediary.

Level III clearances take substantially longer to process because, in addition to the credit, criminal and security indices checks required for all levels of clearance, a field investigation is mandatory. Level III field investigations must cover the preceding 10 years (20 years for a Special Access clearance). Field investigations may therefore involve several cities and provinces and, where reciprocal agreements with allied agencies are in place, foreign countries. Following standards set out in the Government Security Policy (GSP), neighbours, supervisors, co-workers and social acquaintances of an individual are interviewed to verify all aspects of the individual's loyalty to Canada and, so far as it relates to loyalty, the reliability of the individual.

Immigration Screening

Delays: On average, CSIS takes 90 calendar days to perform the security screening of an immigrant. More complex cases may require more thorough checks and investigations. In a tiny proportion of cases, the screening may take between six months and two years.

A new program to streamline immigration processing outside Canada (``profiling'') began abroad on June 1, 1991, but has not yet been studied or evaluated.

Citizenship Screening

We reviewed the performance by the Service of its duty to collect, analyze and retain information about threats to the security of Canada, in the context of the Service's advice to the Secretary of State for Citizenship concerning applicants for Canadian citizenship.

The Security Flag System: In April 1988, a significant and growing case backlog (35,000 unprocessed citizenship applications) prompted a re-examination of the traditional system by which CSIS provides security advice to the Secretary of State. The Service had argued that an assessment of individuals for citizenship purposes was redundant, since a security review had already been done for permanent resident status.

Over several months, consultations between Ministers and officials of CSIS, the Department of Secretary of State, Employment and Immigration and the Privy Council Office achieved a consensus for a new approach to citizenship security screening — the ``Security Flag System".

Under the system, CSIS provides the names, aliases, and biographical data of permanent residents about whom the Service has identified security concerns, thus justifying a closer look at the time of their application for citizenship. The names are provided to the Canadian Employment and Immigration Commission for retention in a special data base under appropriate safeguards.

In processing an application for citizenship, the Citizenship Branch of the Department of the Secretary of State queries this data base to confirm landed status. If an applicant's name has not been ``flagged" by the Service, the Citizenship Branch can assume that a security check with CSIS is not required and can then do the other necessary checks and procedures. If CSIS has flagged the applicant's name, the Citizenship Branch requests security advice from the Service in respect of that applicant. The new system has significantly improved the speed and efficiency of the screening process.

In assessing whether an applicant poses a demonstrable threat to the security of Canada, the Service must apply the ``reasonable belief" test of the *Citizenship Act*. If the Service believes it has sufficient information to meet this test, it sends a ``rejection brief" for review and approval of the Solicitor General before referral to the Department of the Secretary of State.

In other instances, the Service simply informs the Department of the Secretary of State that it possesses insufficient information upon which to sustain a recommendation for denial of citizenship. We found no instances where the Service actually made the Department of the Secretary of State aware of the particulars of its security concerns.

In March 1992, the Citizenship Flag System contained the names of less than 100 Canadian residents. For the month of the review (July 1992) the list contained slightly more than 100 names. For a third of the names on the July list, we examined the documentation that explained their inclusion. The degree of concern expressed by CSIS varied significantly from case to case. We questioned the inclusion of only two names — one because it stemmed from the now discontinued Counter-subversion program and the other because a review of documentation indicated

that the individual might already be a Canadian citizen. The Service has since removed both these names from the list.

Refugee Determination Program Backlog

The Service anticipates requiring another year to complete the review of these cases.

Table 4. Refugee Determination Files

Year	Files Processed
1989-90	7,639
1990-91	29,176
1991-92	20,456

8. Regional Audits

The Committee's research activities have two components. The *CSIS Act* imposes certain responsibilities, such as the ``monitoring'' of exchanges of information with domestic and foreign agencies. We also review issues identified by the public, Parliament or the Minister. Neither of these two functions, however, envisages a systematic review of all CSIS activities.

The Committee provides an opinion each year on the state of Service activities in general. We base our opinion in part on a general audit of all Service operations at one CSIS Regional office. We examine all targeting authorizations, warrant affidavits, approvals pursuant to Ministerial direction, surveillance authorizations and other matters. From among these, we randomly select and audit all aspects of the approval or authorization and any resulting investigation.

We are currently completing the review for 1990-91. Last year, we completed the review for 1989-90, and found the following:

Targeting: Under CSIS policy, no investigation can be conducted at any level without written justification and approval by management.[8]

Overall, the factual basis for the targeting decisions and the decisions themselves raised no problems. We also saw no difficulties with the consequent investigations. However, we were concerned about the extent of access by the Service without warrants to certain types of personal information about targets held by major private institutions. We recommended that the Minister provide clear written guidelines.

Warrants: CSIS prepares affidavits to support applications for warrants. We reviewed these affidavits for factual accuracy and ``balance''. We also examined files on the implementation of warrants, and ``warrant product'' — information derived from authorized warrants — to ensure that the terms of the warrant were followed and that the information obtained was accurate.

In the affidavits we found a few errors, none major. In a few cases, we disagreed with the portrayal of facts and were concerned about the omission of significant contrary information. In one case, however, we applauded the Service for including in the affidavit significant information contrary to the position taken in the application.

[8] For a detailed description of CSIS targeting decision-making process, see: *On Course: National Security for the 1990s: The Government's Response to the Report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act* (Ottawa: Solicitor General Canada, February 1991) at pp. 59-66.

We queried the Service about several matters relating to the execution of warrants and warrant products. We received adequate responses. The Service appears to follow strictly the rules for executing a warrant and processing warrant product, such as solicitor-client privilege. We identified no inaccuracies in the information obtained.

Surveillance: We examined requests for the use of surveillance and the actual use of the surveillance. Surveillance, an art, is part of the mundane, often dull work on which other investigative techniques can build. It provides information about movements, associations and, infrequently, intelligence activities. Surveillance, like any other investigative technique, requires a targeting authorization.

In our review, we found that surveillance was being done only when ``strictly necessary" and that it complied with CSIS policies. All those investigated were legitimate targets. We did note that surveillance results in the collection of significant amounts of personal information (for example, about people's associates), but we found no substantive problem with its collection.

Ministerial directions: Ministerial directions regulate matters such as campus investigations and operations with allied agencies. A recent Ministerial direction covers ``sensitive institutions". We noted that almost two-thirds of the operations requiring Ministerial approval involved (often only in a very limited way) educational or religious institutions. In general, we were satisfied with the respect shown for the integrity of these institutions. There were no unnecessary investigations involving them. In one instance, however, we recommended that the Minister examine and approve a sensitive operation annually, should it continue. The Solicitor General had approved it five years ago, and the operation had perhaps been forgotten at CSIS Headquarters.

9. Review of General Matters

Task Force

In March 1992, the Solicitor General told Parliament that he had asked the Director of CSIS to give him ``an assessment of how the security environment might affect the Service's mandate over time''. He also announced the formation of a task force in CSIS to prepare the assessment. The Director later informed us that he expected the task force report to be available in the Fall.

Ministerial Direction

The *CSIS Act* requires the Committee to review direction provided by the Solicitor General to the Service under subsection 6(2) of Act. Ministerial direction governs certain types of CSIS investigations in potentially sensitive areas, such as investigations on university campuses. Many Ministerial directions require that the operations they address be approved by the Minister.

The Committee examines Ministerial directions from several angles. It receives and analyzes related directions issued by the Service. It examines the implementation of directions in specific cases. It also looks for significant changes in the number of operations that require Ministerial approval.

The Committee's concern includes, but is not focused on, compliance: whether the directions are being followed. Compliance is a primary focus of the Inspector General. The Committee's major concern is to identify poor Ministerial direction or lack of compliance with direction that may lead to improper behaviour or violations of the *CSIS Act*.

One important Ministerial Direction concerning threats to the security of Canada and operational definitions was referred to in last year's Annual Report. This Ministerial Direction was issued in lieu of the amendments to the *CSIS Act* itself that were recommended by the Thacker Committee. CSIS is bound by Ministerial direction in the same way as it is bound by the *CSIS Act*, but, of course, Ministerial Direction can be withdrawn or amended as future Ministers see fit. The Direction is included as Annex E to this report.

This year, the Committee received copies of three new Ministerial directions. One concerns the collection, retention and disclosure of communications intercepted under Federal Court warrants. It deals with the retention of tapes for use in potential criminal prosecutions. It also contains provisions protecting third party and solicitor-client communications.

The second is a synopsis of the annual direction from Cabinet entitled ``National Requirements for Security Intelligence for fiscal year 1991-92''. The former Solicitor General revealed that ``national interests'' are unchanged from 1991. They are:

(a) public safety

(b) integrity of the democratic process

(c) security of government assets

(d) international peace and stability

(e) economic security

The National Requirements, the means to achieve the national interests, vary significantly from last year. Some changes are easy for the Committee to support. For example, greater emphasis is placed on determining the nature of the threat following the ``transformation in East-West relations". The direction stresses new threats, such as the proliferation of destabilizing military technologies. We will examine this issue fully in the autumn of 1992.

The Committee has had some difficulty, however, with other changes to the National Requirements. The 1991-92 National Requirements place greater emphasis on protection of economic assets and Canadian scientific and technological expertise. This is a response to what is cited as ``the projected shift in foreign espionage in Canada from the political-military to the political-economic sphere".

CSIS and allied intelligence services appear to be changing their definitions of ``national security" to put greater emphasis on the protection of national economic interests.

A third Ministerial direction concerns the hiring of CSIS employees. It replaces an earlier direction that CSIS inform the Minister of the hiring of ex-RCMP officers. The new direction instructs the Service to inform the Minister of general personnel management policies and activities.

CSIS Operational Manual

The CSIS Operational Manual interprets Ministerial direction and provides general instruction for daily use by CSIS Intelligence Officers. The two volume set contains all the rules for CSIS investigations, and includes reference chapters and ``bulletins". SIRC has a copy of the Manual, and receives updates.

The Committee examines changes to the Manual as if they were changes to Ministerial direction. The Committee reviews all changes to the Manual, and almost all Committee studies begin with an examination of relevant parts of the Manual.

In 1991-92, the Service made eleven changes to the Manual. One new chapter was added, covering procedures for implementing the new Government Security Policy on security screening. The chapter contains provisions on the collection and retention of security screening information. One bulletin deals with access to the Canadian Police Information Centre (CPIC) data base. It

includes clauses dealing with the protection of personal information and the logging of access requests, and specifies which data banks CSIS can access directly. For example, CSIS does not have direct access to the CPIC *Young Offenders Act* data base. Other amendments to the Manual cover administrative and investigative matters.

In last year's Annual Report, the Committee noted the need for ``comprehensive guidelines on the use of [the Service's] most intrusive powers'' (page 4). One bulletin released in 1991-92 deals with the implementation of powers approved for use by Federal Court warrants. This item is billed by the Service as a replacement for the now defunct Technical Aids Policies and Procedures Manual. Bulletin by bulletin, the Service is putting together a full set of instructions for the use and processing of warrants. However, the process is not yet complete.

Each year we ask for an update on the progress made by CSIS in updating sections of the CSIS Operational Manual that were prepared before July, 1984, when the *CSIS Act* came into force. The Service told us that in 1991-92 it focused its development resources on core policies such as targeting, disclosure and cooperation with domestic agencies and allied services. We were told that when these projects are completed, the Service will attend to ancillary policies and other dated material.

Disclosures in the Public Interest

Under section 19 of the *CSIS Act*, the Director must report to the Committee any disclosures of information to Ministers or public servants that CSIS makes in the public interest. There were no reports of public interest disclosures under section 19 during 1991-92.

Regulations under Subsection 8(4) of the *CSIS Act*

Subsection 8(4) of the *CSIS Act* gives the Governor in Council the power to make regulations concerning employment conditions. No such regulations were introduced in 1991-92.

Investigations under Paragraph 2(d) of the *CSIS Act*

Ministerial direction requires the Minister to approve targeting authorizations under paragraph 2(d) of the *CSIS Act*. The Minister approved no such authorizations during the 1991-92 fiscal year.

Report of the Director and Certificate of the Inspector General

The *CSIS Act* directs the Committee to examine the Report of the Director of CSIS to the Solicitor General, and the Certificate of the Inspector General, which is also provided to the Solicitor General.

The Committee generally reports on activities occurring in the past fiscal year. Unfortunately, the Director's report usually arrives in late July or August, when the Committee's report is being put into final form. The Certificate of the Inspector General reaches us still later, in August or September.

The Director's report provides a useful update and overview of CSIS activities for the Committee. In addition, we obtain from the report some of the statistics we use in preparing our data base on ``operational activities'', as required by section 38 of the Act. However, the report is not a significant tool for our audit of CSIS activities.

In his 1991 Certificate, the Inspector General indicated that the 1991 CSIS Annual Report had weaknesses of fact and analysis that undermined its usefulness. Furthermore, the report ``failed to demonstrate how CSIS had responded to government priorities''.

The Inspector General noted that it was impossible for him to keep abreast of all CSIS activities in a given year. Accordingly, the Certificate was not ``a certification of CSIS's entire operations in 1990-91''. In the Certificate, the Inspector General informed the Minister of three instances of non-compliance with Ministerial direction or the *CSIS Act*, and one instance of a lapse in Service reports to the Minister.

Inspector General's Reports and Studies

Most of the Inspector General's reports are prepared on behalf of the Minister. However, section 40 of the *CSIS Act* also authorizes us to ask the Inspector General to conduct reviews. We discuss our work plan with the Inspector General every year to ensure that our respective programs do not lead to duplication.

In 1991-92, the Committee received one study by the Inspector General on the exchange of information and intelligence between CSIS and the Communications Security Establishment (CSE), and one on threat assessments. In last year's Annual Report, we described these reviews. We received the final reports in October 1991 and January 1992 respectively.

The Committee and the Inspector General both closely examine the factual accuracy and balance in CSIS affidavits sworn to support warrant applications. In December 1991, the Inspector General gave the Minister a report on five warrant affidavits and the CSIS internal quality control procedures for the warrants. According to the Inspector General, some affidavits contained errors,

one presented some information in an unbalanced fashion, and some contained statements of belief expressed as facts.

On June 30, 1992, we received a top secret report from the Inspector General on the activities of two CSIS units involved in the planning and implementation of warrant operations. The report found that the employees of the units displayed a high degree of professionalism and dedication. The Inspector General also concluded, however, that formal CSIS policies in this area were outdated, incomplete and, in places, confusing. When the Inspector General's review was near completion, CSIS issued policy dealing with various aspects of warrant operations. The new policy addressed some, but not all, of the Inspector General's concerns.

The Inspector General found that although the planning and implementation units did not contravene any laws or Ministerial directions, in one sensitive operation Service personnel failed to report in a timely way to the Solicitor General.

Special Reports

Under section 54 of the *CSIS Act*, we can make special reports to the Solicitor General on any matter relating to the performance and functions of the Service. In 1991-92, we submitted three studies to the Minister under section 54. All mentioned certain concerns and made recommendations:

- *Exchange of Information and Intelligence between CSIS & CSE, Section 40 Study*, October 1991 (TOP SECRET)
- *Threat Assessments, Section 40 Study*, January 1992 (SECRET)
- *The Attack on the Iranian Embassy in Ottawa*, May 1992 (TOP SECRET)

A list of SIRC reports and studies is attached as Appendix B.

SIRC Consultations and Inquiries

Formal inquiries: As part of our review function, we directed 178 formal inquiries, not counting inquiries arising out of complaints, to the Service in the 1991-92 fiscal year. CSIS took an average of 58 days to answer a formal inquiry.

Briefings: We met with the Director three times during the fiscal year — on December 12, 1991, and on February 12 and March 18, 1992. We visited CSIS regional offices when our regular meetings took us out of Ottawa. We were briefed on regional operations in Toronto on March 11, 1992, in Halifax on May 20 and in Vancouver on June 22.

Beyond CSIS: The Chairman met with the Minister of Justice on August 12, 1991, and with the Solicitor General and Deputy Solicitor General on August 13. On both occasions he discussed the possibility of SIRC opening an investigation into the ``Air India'' incident. On February 12, 1992, the Committee met with the Auditor General and two of his officials. In May 1992, the Chairman travelled to London, England to meet with the newly appointed head of MI-5, Stella Rimington.

Unlawful Acts by CSIS Employees

Under section 20 of the Act, the Director must advise the Solicitor General when he believes that a CSIS employee has acted unlawfully. As required by subsection 20(4), we receive a copy of the Director's report and any comments made by the Solicitor General to the Attorney General.

We received one report under section 20 in 1991-92 that referred to an incident which occurred in the previous fiscal year. In 1990, a CSIS employee may have intercepted private communications without proper authorization, contrary to section 184 of the *Criminal Code* and sections 21 and 22 of the *CSIS Act*. Other employees may have been parties to this act, also a criminal offence. The actions arose from a misunderstanding concerning the application of a warrant.

The duration of the interception was very brief and all recordings were erased. The Director indicated that to prosecute in this case would be injurious to national security. The Solicitor General accepted his assessment.

10. Inside CSIS

Review of the Security Intelligence Environment

In Chapter 9 we described the work of the Director's task force on the security intelligence environment. We will comment on its report in our next annual report.

Polygraph Testing

Starting with our 1985-86 Annual Report, we have criticized the way CSIS uses the polygraph in seven consecutive reports. We continue to doubt the accuracy of polygraph examinations and their validity in security screening programs. The error rate of the test (ten per cent or more), combined with the test's perceived scientific legitimacy, creates too high a risk of serious injustice to a person who appears to have the intent to deceive or whose test results appear inconclusive. We believe the polygraph is given more weight than its reliability warrants.

In our 1985-86 Annual Report, we called on the government to evaluate the polygraph process objectively. We later learned that an outside consultant would do a study for CSIS. Ultimately, however, the study failed to evaluate the polygraph. As we mentioned in our last annual report, it was not even evident that the consultant had analyzed the test results which CSIS had been collecting for at least seven years.

CSIS currently uses the polygraph as one tool to assess the ``loyalty'' of all CSIS applicants. We have argued before that rigorous security screening would eliminate the need for this fallible polygraph process.

The volume and scope of testing during 1991-92 changed little from the last fiscal year. What has changed is the process. CSIS responded to last year's report by the outside consultant, implementing the recommendations. The changes ostensibly provide for a more informed subject and a standard test procedure. For example, the procedures now require early notification of the requirement to take the test, early provision of questions, and a uniform interview script.

We long feared that polygraph examinations would be expanded government-wide for higher security jobs. This could lead to an erosion of an equitable basis for the security screening of many more persons. We have since learned that almost all federal government agencies have no interest in using the polygraph for security screening. Therefore, concern over the proliferation of polygraph testing in the federal government seems unfounded at present. Applicants for CSIS jobs, however, continue to be subjected to a security screening tool that most democracies have rejected.

The polygraph issue was brought to the Interdepartmental Committee on Security and Intelligence. That Committee referred the issue back to the Ministry of the Solicitor General, which has responsibility for CSIS. The Solicitor General has written to the Director of CSIS in support of the policy to use the polygraph, subject to certain conditions, for the pre-employment

screening of new entrants.

Recruitment

The CSIS Training Centre held two Intelligence Officer Entry Training Classes in fiscal year 1991-92. There were 49 new recruits. Only two of the 49 came from other positions in the Service.

In past reports we discussed equitable representation and the steady progress made towards increasing the number of women in the ranks. In the first Intelligence Officer category (IO-01), there were 48 per cent male and 52 per cent female employees as of March 31, 1992. In the more senior IO-02 category, there were 54 per cent male and 46 per cent female employees. In the still more senior IO categories, however, men still greatly outnumbered women. Accordingly, the IO category as a whole is 80 per cent male and 20 per cent female. Clearly, however, CSIS is making every effort to remedy the gender imbalance by ensuring that approximately equal numbers of men and women are recruited into the IO category.

Women make up approximately 10 per cent of the management category in the Service.

Bilingualism

On July 1, 1991, CSIS implemented new official language policies which allowed enhanced access to second language training. CSIS will also undertake a review of all bilingual positions. The goal is to ensure that the only positions designated as bilingual are those with practical and realistic second language needs, as defined by the *Official Languages Act* and the Service's new policies.

Public Relations

The Director of CSIS met with members of the editorial board of the Ottawa *Citizen* on April 30, 1991, and was interviewed by Southam News on February 25, 1992. In addition, the Solicitor General tabled the first public CSIS annual report on March 19, 1992.

Accommodations

Phase I of the new National Headquarters project has been completed and costs remain under budget. Excavation and foundation work began on Phase II in November 1991. No date has yet been set for completion.

Finances

In our 1990-91 Annual Report, the Committee assessed the budget increases of the Service since 1985-86. For fiscal year 1992-93, the budget for CSIS is set at $215.6 million, an increase of 2% over 1991-92. The CSIS budget for 1992-93 reflects a mixture of cuts in certain areas to compensate for additional expenditures in others. The expected increases are not related to expanded operational activity. CSIS will allocate a major part of the additional funds for new facilities in B.C. Region and for CSIS Headquarters in Ottawa.

Table 5. CSIS Budget

Total Estimates (in thousands)	
1985-86	$115,908
1986-87	$132,844
1987-88	$136,861
1988-89	$157,852
1989-90	$165,417
1990-91	$205,325
1991-92	$211,229[9]
1992-93	$215,588

In November 1991, we discussed funding and resource use in CSIS. The financial data received by the Committee, however, is limited and we are not in a position to judge whether increases received by the Service are justified. In the spring of 1992, the Committee met with the Auditor General. We have agreed to await the findings of the Auditor General before taking any further action.

[9] 1991-92 Main Estimates reduced by $2,722,000 for Government Deficit Reduction Initiatives program.

11. Inside SIRC

Accounting to Parliament

On October 4, 1991, the Solicitor General tabled the Committee's 1990-91 Annual Report. A news conference followed. The Committee appeared before the House of Commons Sub-committee on National Security on November 19, 1991, to answer questions on the Annual Report. Two new Committee members, the Hon. E. Jacques Courtois, P.C., Q.C., and the Hon. Michel Robert, P.C., Q.C., appeared before the Sub-committee on April 1, 1992 to answer questions about their appointments to SIRC the previous December. On May 13, 1992, the Chairman and Mr. Courtois appeared before the Sub-committee to answer questions about our 1991-92 estimates.

Staying in Touch

On November 20, 1991, the Hon. Jean Jacques Blais, P.C., Q.C., addressed the Royal Kingston United Services Institute in Kingston, Ontario. This is an organization of retired officers from the Canadian Armed Forces and the RCMP.

We helped fund the 1991 conference of the University of Toronto Department of History, held in Toronto on November 7-9, 1991. The focus of the conference was ``Espionage: Past, Present, Future''.

We completed planning for a seminar to be held on September 23, 1992 in Montreal. Parliamentarians, academics, lawyers and others will discuss ``Where does CSIS go from here, now that the Cold War is over''.

Spending

Our 1991-92 budget is set out in Table 6. At $1,568,000, it represents an increase of four per cent from the budgeted spending of $1,505,000 in 1990-91. Our 1992-93 estimate of $1,541,000 represents a decrease of two per cent from the 1991-92 budget.

Table 6. SIRC Budget 1991-92		
Personnel		$805,000
Salaries and wages	697,000	
Contributions to employee benefit plans	108,000	
Goods and Services		754,000
Professional and special services	597,000	
Other	157,000	
Total Operating Expenditures		1,559,000
Capital Expenditures		9,000
Total		1,568,000

Source: 1992-93 Estimates, Part III, Section II, figure 7

Personnel

The Committee has a staff of fourteen: an Executive Director, a Senior Complaints Officer to handle complaints, ministerial reports, and research; a Director of Research (Counter-Terrorism); a Director of Research (Counter-Intelligence); four Research Officers; an Executive Assistant who co-ordinates activities on behalf of the Chairman, conducts all media liaison, co-ordinates the production of the annual report, and undertakes research projects; an administrative officer who is also the Committee Registrar, and an administrative support staff of four. The administrative support staff have a particularly heavy burden because the materials handled by the Committee are sensitive and highly classified, and must be dealt with using special security procedures.

At its regular monthly meetings, the Committee sets its research and related priorities. Day-to-day operations are delegated to the Executive Director, with direction if necessary from the Chairman in his role as Chief Executive Officer of the Committee.

A. Glossary

ARAACP	— Airport Restricted Area Access Clearance Program
BCCLA	— British Columbia Civil Liberties Association
CAF	— Canadian Arab Federation
CAUT	— Canadian Association of University Teachers
CI	— Counter-Intelligence
CMC	— CSIS Crisis Management Centre
CNN	— Cable News Network
COMMITTEE	— Security Intelligence Review Committee (SIRC)
CPIC	— Canadian Police Information Centre
CSE	— Communications Security Establishment
CSIS	— Canadian Security Intelligence Service
CT	— Counter-Terrorism
DIRECTOR	— the Director of CSIS
DND	— Department of National Defence
GOI	— Government of India
GSP	— Government Security Policy
IO	— Intelligence Officer
IPC	— Intelligence Production Committee
MEK	— Mujahedin-E-Khalq
MINISTER	— the Solicitor General of Canada, unless otherwise stated
MOSSAD	— Israeli Secret Intelligence Service
MOU	— Memorandum of Understanding
RAP	— Analysis and Production Branch
RCMP	— Royal Canadian Mounted Police
RENAMO	— Portuguese acronym for Mozambican National Resistance
R & D	— Research and Development
SERVICE	— Canadian Security Intelligence Service (CSIS)
SIRC	— Security Intelligence Review Committee
SIU	— Special Investigation Unit (DND)
SLO	— Security Liaison Officer

TAPP — Technical Aids Policies and Procedures (CSIS)

TARC — Targeting Approval and Review Committee

B. SIRC Reports and Studies since 1984

(Section 54 reports — special reports the Committee makes to the Minister — are indicated with an *)

Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues, April 14, 1986 (139 pages/SECRET) * (86/87-01)

Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service, May 1986 (SECRET) ***** (86/87-02)

The Security and Intelligence Network in the Government of Canada: A Description, January 1987 (61 pages/SECRET) ***** (86/87-03)

Closing the Gap: Official Languages and Staff Relations in the CSIS, June 1987 (60 pages/UNCLASSIFIED) ***** (86/87-04)

Ottawa Airport Security Alert, March 1987 (SECRET) ***** (86/87-05)

Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions, May 1987 (SECRET) ***** (87/88-01)

Counter-Subversion: SIRC Staff Report, August 1987 (350 pages/SECRET) (87/88-02)

SIRC Report on Immigration Screening, January 1988 (32 pages/SECRET) ***** (87/88-03)

Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement, March 1988 (18 pages/PUBLIC VERSION) *****(87/88-04)

The Intelligence Assessment Branch: A SIRC Review of the Production Process, September 1988 (80 pages/SECRET) ***** (88/89-01)

SIRC Review of the Counter-Terrorism Program in the CSIS, November 1988 (300 pages/TOP SECRET) ***** (88/89-02)

Supplement to SIRC Report on Immigration Screening (January 1988 1989), November 1989 (SECRET) ***** (89/90-01)

Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS, April 1989 (40 pages/SECRET) ***** (89/90-02)

SIRC Report on CSIS Activities Regarding the Canadian Peace Movement, June 1989 (540 pages/SECRET) ***** (89/90-03)

A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information, August 1989 (SECRET) (89/90-04)

Report to the Solicitor General of Canada on Citizenship/Third Party Information, September 1989 (SECRET) ***** (89/90-05)

Amending the CSIS Act: Proposals for the Special Committee of the House of Commons, September 1989 (UNCLASSIFIED) (89/90-06)

SIRC Report on the Innu Interview and the Native Extremism Investigation, November 1989 (SECRET) ***** (89/90-07)

A Review of the Counter-Intelligence Program in the CSIS, November 1989 (700 pages/TOP SECRET) ***** (89/90-08)

Security Investigations on University Campuses, February 1991 (TOP SECRET) ***** (90/91-01)

Release of Information to Foreign Agencies, January 1991 (TOP SECRET) ***** (90/91-02)

Domestic Exchanges of Information, September 1990 (SECRET) ***** (90/91-03)

Regional Studies (six studies relating to one region), October 1990 (TOP SECRET) (90/91-04)

Investigations, Source Tasking and Information Reporting on 2(b) Targets, November 1990 (TOP SECRET) (90/91-05)

Section 2(d) Targets — A SIRC Study of the Counter-Subversion Branch Residue, September 1990 (SECRET) (90/91-06)

CSIS Activities Regarding Native Canadians — A SIRC Review, January 1991 (SECRET) ***** (90/91-07)

Report on Multiple Targeting, February 1991 (SECRET) (90/91-08)

Study of CSIS' Policy Branch, October 1990 (CONFIDENTIAL) (90/91-09)

Review of the Investigation of Bull, Space Research Corporation and Iraq, May 1991 (SECRET) (91/92-01)

Report on Al Mashat's Immigration to Canada, May 1991 (SECRET) ***** (91/92-02)

CSIS and the Association for New Canadians, October 1991 (SECRET) (91/92-03)

Exchange of Information and Intelligence between CSIS & CSE, Section 40 Study, October 1991 (TOP SECRET) * (91/92-04)

Victor Ostrovsky, October 1991 (TOP SECRET) (91/92-05)

Report on Two Iraqis — Ministerial Certificate Case, November 1991 (SECRET) (91/92-06)

Threat Assessments, Section 40 Study, January 1992 (SECRET) *****(91/92-07)

East Block Investigations, August 1991 (TOP SECRET) (91/92-08)

Review of CSIS Activities Regarding Sensitive Institutions, August 1991 (TOP SECRET) (91/92-10)

A SIRC Review of CSIS' SLO Posts (London & Paris), September 1992 (SECRET) (91/92-11)

The Attack on the Iranian Embassy in Ottawa, May 1992 (TOP SECRET) ***** (92/93-01)

C. Complaints Case Histories

The following are brief outlines of complaints on which SIRC reached decisions in 1991-92. All are complaints launched under section 41 of the *CSIS Act*. Complaints that were withdrawn or resolved before the Committee completed its investigations, or that were beyond its jurisdiction, are not reviewed here.

Applications for Accreditation

After filing personal information requests with the RCMP under the *Privacy Act*, two complainants learned of problems with their applications for accreditation to work at an international event being held in Canada. One person's application for accreditation had been denied, while the other's had been revoked. In both cases, the RCMP had acted ``as a result of information received from CSIS''.

Both individuals submitted their complaints to the Director of CSIS but were not satisfied with his response. They then turned to the Committee, which decided to conduct an investigation and hearing.

One Committee member heard both complaints. The Committee and all counsel involved agreed that proceeding in this way caused no prejudice to the complainants. In fact, counsel representing both complainants had submitted their complaints together, and the facts giving rise to the complaints were substantially similar.

At the request of CSIS counsel, and after hearing evidence from a witness and arguments from all counsel, the Committee ordered the complainants and their counsel excluded from hearing certain evidence.

The Committee recognized that this would limit the complainants' *prima facie* right to full disclosure. It decided, however, that the public interest in non-disclosure justified the prejudice to the complainants. To compensate, the Committee ordered that, to the extent that national security considerations permitted, they receive written summaries of all *in camera* evidence and that their counsel be given a right to cross-examine on that evidence. The Committee also instructed the Committee's counsel to cross-examine the respondent's witnesses vigorously during the *in camera* proceedings.

The Committee could focus only on the activities of CSIS. It had no authority to review the actual decisions to deny or revoke the complainants' accreditations, as these decisions were made by the RCMP, not CSIS.

The Committee concluded that CSIS had acted properly in passing information to the RCMP under paragraph 19(2)(a) of the *CSIS Act*. However, the Committee also found that the way CSIS conveyed the information to the RCMP appeared to have a number of deficiencies. It also found that CSIS had failed to exercise its discretion responsibly and professionally.

Admission to Canada of Alleged Terrorist

A second section 41 complaint related to the admission to Canada in 1986 of an alleged one-time representative of the Mozambican National Resistance (RENAMO).[10] The complainant had complained to the Director of CSIS about the security screening performance of CSIS in this case,[11] but was not satisfied with the Director's response.

The Committee's investigation focused on how CSIS performed its duties and functions in immigration security screening. In this case, the Committee had no authority to investigate the decision allowing the individual to enter into and remain in Canada.[12] (Had the case come to the Committee under section 39 of the *Immigration Act, 1976*, the Committee could have investigated a decision allowing the individual to enter). The Committee's role was simply to decide whether the CSIS activities aimed at providing security advice were proper and adequate.

To assess the performance of CSIS, the Committee member closely examined the state of knowledge of the External Affairs Social Affairs Officer,[13] the CSIS Security Liaison Officer[14] and persons outside government about the goals, objectives and activities of RENAMO in 1986.

---

[10] RENAMO is the Portuguese acronym. In 1986, RENAMO was a terrorist organization.

[11] In accordance with section 14 of the *CSIS Act*, CSIS conducts security screening of and advises the Minister of Employment and Immigration on inadmissible immigrant applicants, as defined in paragraphs 19(1)(e), (f) and (g) of the *Immigration Act, 1976*.

[12] In 1986, the decision to grant or refuse permanent residence status in Canada rested with the Minister of Employment and Immigration. In effect, the Department of External Affairs was responsible for the delivery of the Immigration Program outside Canada. It was accountable to Employment and Immigration Canada for complying with the *Immigration Act* and regulations and related policies in all matters related to visa issuance overseas and for meeting a quota of landings of immigrants selected abroad.

[13] In 1986, Social Affairs Officers were foreign service officers employed by the Department of External Affairs. Their duties were to implement certain provisions of the *Immigration Act*, interview applicants for all categories of visas and determine whether applicants met the requirements of the *Immigration Act* and regulations.

[14] Security Liaison Officers are posted abroad with the CSIS Foreign Liaison Unit.

The Committee concluded that interviews conducted by Security Liaison Officers abroad could identify security concerns only if the Officers were well-informed and conducted the interview skillfully. Otherwise, the screening process would be seriously compromised. The Committee concluded that both CSIS Headquarters and the Security Liaison Officer involved were inadequately prepared to review an application by an alleged representative of RENAMO.

The Committee did not (and had no authority to) consider the decision of the Minister of Employment and Immigration to admit the alleged RENAMO member to Canada. It acknowledged that even if publicly available information about RENAMO had been properly communicated to the Security Liaison Officer, the final outcome might have been no different

D. Montreal Seminar (September 1992)

We invited guests, including lawyers, scholars and parliamentarians, to attend a September 23, 1992 seminar on ``Where does CSIS go from here, now that the Cold War is over''. The Committee is grateful to them for their contribution to its thinking on the topics discussed.

Mr. Murray Rankin
Barrister and Solicitor
Array & Finlay
Victoria, B.C.

Mr. Alan Borovoy, O.C., Q.C.
General Counsel
Canadian Civil Liberties
Association
Toronto, Ontario

M. Jean-Paul Brodeur
Directeur
Centre international de
criminologie comparée
Montreal, Quebec

Mr. Ray Protti
Director
CSIS
Ottawa, Ontario

Mr. Simon Noël
Lawyer
Noël, Berthiaume, Aubry
Hull, Quebec

Mr. Richard Mongeau
Lawyer
Mongeau, Gouin, Côté, Roy
Montreal, Quebec

Mr. Joseph Nuss
Lawyer
Ahern, Lalonde, Nuss, Drymer
Montreal, Quebec

Ottawa, Ontario

Mr. Jean-F. Keable
Lawyer
Grondin, Poudrier, Bernier
Quebec, Quebec

Mr. Raymond Royer
President
Bombardier Inc.
Montreal, Quebec

Prof. Franklyn Griffiths
Dept. of Political Science
University of Toronto
Toronto, Ontario

Prof. C.E.S. Franks
Queen's University
Department of Political
Science
Kingston, Ontario

Mr. Derek Lee, M.P.
House of Commons
Ottawa, Ontario

Mr. Tom Wappel, M.P.
House of Commons
Ottawa, Ontario

Mr. Ken Atkinson, M.P.
Houses of Commons
Ottawa, Ontario

Mr. Phil Rosen
Senior Analyst
Research Branch
Parliamentary Library

Mr. Tom Bradley
Director General
Secretariat

CSIS
Ottawa, Ontario

Mr. Joseph S. Stanford, Q.C.
Deputy Solicitor General
Ministry Secretariat
Ottawa, Ontario

Ms. Wendy Porteous
Ass't Deputy Solicitor General
Police & Security Branch
Ottawa, Ontario

Ms. Ursula Menke
Inspector General of CSIS
Ottawa, Ontario

Mr. Michael de Rosenroll
Ass't Inspector General (Policy & Standards)
Ottawa, Ontario

Glenys Parry
Ass't Inspector General (Operations)
Ottawa, Ontario

E. Ministerial Direction Defining Threats to the Security of Canada

Last year we reported that the Minister had issued one direction to CSIS. It interpreted such elusive terms as ``threats to the security of Canada", ``espionage and sabotage" and ``foreign influenced activities" more precisely than does section 2 of the *CSIS Act*.

Writing to the Director, the Minister explained the purpose of the direction:

> This direction is intended to provide guidance in respect of the operational interpretation of terms found in section 2 of the *CSIS Act*, and general policy framework to govern the Service's conduct of its security intelligence activities under section 12.

The text of the direction is set out below:

Section 2
Threats to the Security of Canada

The primary mandate of the Service is to provide information and advice to the Government on the activities described in section 2 of the *Act*, in as timely and accurate a manner as possible.

Section 2 of the *Act* defines ``threats to the security of Canada" to include espionage or sabotage, foreign influenced activities, the threat or use of acts of serious violence for political purposes, and activities directed toward undermining or overthrowing Canada's constitutionally established system of government. Each, in turn, is accompanied by important qualifications.

In enacting the threat definitions of section 2, Parliament sought to provide the Service with sufficient scope and flexibility to perform its duties and functions effectively, while protecting the rights and freedoms of individuals to the fullest extent possible. This direction, including the Annex, is intended to guide the Service in employing the terms of section 2 in a manner which is consistent with the intent of the *Act* and the *Charter*, without expanding the scope and content of section 2 itself. It is also intended to ensure that the Service and its client, the Government of Canada, share a common understanding and approach to the terms of section 2. Should this guidance inhibit the Service's ability to fulfil its mandate, I would expect to be advised accordingly.

The operational interpretations in question are to be found in the Annex to this letter.

Section 12
Collection, Analysis, Retention, Reports and Advice

Environmental Scanning

The Service has a general responsibility to keep itself well informed concerning the political, social and economic environment from within which threats to the security of Canada may emerge. Such information may be obtained from open or unsolicited sources and is intended to assist the Service in observing trends or identifying patterns which may suggest the development of a threat. Environmental scanning of this sort should complement and inform the Service's investigative activities. Where appropriate, information from environmental scanning should be integrated with information obtained from investigative activities under section 12 to provide the most accurate threat assessment available and correspondingly to advise the Government.

The Service is to exercise acute vigilance to ensure that its environmental scanning activities are not used for the purpose of investigating individuals, groups or organizations under section 12.

Collection

As an agency mandated by statute to carry out the full intelligence cycle of collection, analysis, retention, reporting and advice, the Service should ensure that an appropriate balance is maintained between the collection and remaining functions, and that the powers associated with these functions are exercised in a reasonable manner.

Collection under section 12 must be for the purpose of collecting information and intelligence ``by investigation or otherwise'' on activities which may reasonably be suspected of constituting threats to the security of Canada. In this context, the term ``or otherwise'' should be understood to include the receipt of unsolicited information including information obtained from foreign, domestic and open sources that meet the test for collection.

The Service should focus its collection activities in accordance with my annual direction on National Requirements for Security Intelligence which specifies, within the scope of the threat definitions, those aspects of Canada's security about which the Government is currently most concerned. The Service should also routinely consult with other Departments and Agencies concerning their specific security intelligence requirements and on activities detrimental to Canada's interest.

The Service is to accord priority to the collection of information on those activities directly ``against Canada" or ``within Canada."

Reasonable Grounds to Suspect

Prior to the collection of any information under section 12, the Service needs ``reasonable grounds to suspect" that the targeted activities constitute threats to the security of Canada. In order to meet the test for ``reasonable grounds to suspect," the Service must employ an objective standard, namely the existence of demonstrable grounds for suspicion. These should include:

- factual grounds; or
- credible allegations; and
- reasonable deduction from these facts or credible allegations.

The Service should ensure that it documents its grounds.

Lawful Advocacy, Protest or Dissent

Lawful advocacy, protest or dissent may not be investigated unless such activities are carried on in conjunction with threats referred to in section 2. In such circumstances, the Service must carefully weigh the requirement for an investigation against the potential impact of its investigation on the civil liberties of individuals or the most sensitive institutions of our society, as required by the Ministerial direction on the conduct of investigations.

Strictly Necessary

The *CSIS Act*, consistent with the *Charter*, is based on the principle that the State should not interfere with the privacy of individuals unless and only to the extent that there are valid reasons to do so. This means that the Service should target only those threatening activities about which the Government needs to be informed. The determination by the Service of which activities warrant a collection effort will depend on the Service's professional assessment of the potential seriousness of a threat.

The nature and extent of the collection must be governed by the ``strictly necessary" test. The Service should collect only the kind and amount of information that is strictly necessary to provide the Government with complete, accurate and timely information and advice.

When the Service has determined that an activity should be investigated, it should ensure from the outset that the investigative means chosen, and the way these means are employed, are reasonable under the circumstances. The Service must ensure that the scope and intrusiveness of its collection activities are proportionate to the seriousness of the threat being investigated.

Analysis

The collection and analysis functions of the Service should work toward common goals, based on the National Requirements for Security Intelligence. Analysis should play a fully integrated role in all of the significant activities of CSIS. The Service should continue its efforts to ensure that the analysis function operates as a full partner with the collection/investigation function.

The Service should continue to subscribe to the most rigorous standards of analysis and advice. Where it is known that an intelligence report may be instrumental in denying any benefit or material advantage, including employment, senior level approval should be secured prior to transmittal.

Retention

Section 12 provides the Service with the authority to retain information and intelligence consistent with its mandate. This is an essential function for the operational effectiveness of the Service. It should be a Service priority to continue to develop a comprehensive and practical system for the review, at reasonable intervals, of all investigative files collected under the authority of section 12. This process is required to remove from operational files information whose retention may no longer be reasonable or necessary. In due course, I will be issuing Ministerial direction on this question.

Report to and Advise the Government of Canada

In the final analysis, the Service's effectiveness will be judged on the basis of the quality and timeliness of its reports and advice. The Service's principal clients should be those Ministers and officials with statutory or other responsibilities related to the security of Canada. The provision of reports and advice to the RCMP, given its duties and functions under the *Security Offences Act*, should be a primary reporting responsibility of the Service.

The Service must ensure that it satisfies clients requiring both ``operational'' and ``strategic'' intelligence. With respect to strategic intelligence, the Service should continue to work closely with both the Intelligence Advisory Committee and the Security Advisory Committee.

As the Minister accountable for security matters, I expect to be kept fully informed on all Service activities which bear on my responsibilities as Solicitor General.

I am providing a copy of this direction to the Chairman of SIRC in accordance with the terms of subsection 6(2) of the *CSIS Act*.

Annex

Section 2 — Operational Interpretations

Espionage and Sabotage

``Espionage'' activities are those which are conducted for the purpose of acquiring by unlawful or unauthorized means information of assets relating to sensitive political, economic, scientific or military matters, or for the purpose of their unauthorized communication to a foreign state or foreign political organization.

``Sabotage'' activities are those which are conducted for the purpose of endangering the safety, security or defence of vital public or private property, such as installations, structures, equipment or systems.

Foreign influenced activities

``Foreign influenced activities'' are those directed, controlled, financed or otherwise significantly affected by a foreign state or organization, their agents or others working on their behalf.

Acts of serious violence for the purpose of achieving a political objective

``Acts of serious violence'' are those that cause grave bodily harm or death to persons, or serious damage to or the destruction of public or private property; and are contrary to Canadian law or would be if committed in Canada. These would not include acts of minor violence with political overtones.

In the case of acts of violence for political purposes, the Service should restrict its investigations to the threat or use of acts of violence which it determines to be ``serious.''

Activities directed towards undermining or overthrowing Canada's constitutionally established system of government

Activities directed towards undermining or overthrowing Canada's constitutionally established system of government are those seeking to interfere with or ultimately destroy the electoral, legislative, executive, administrative or judicial processes or institutions of Canada.

``...against Canada''

Espionage or sabotage is ``against Canada'' when such activities are directed against the information or assets of the Government of Canada, or are otherwise intended to cause injury to or interfere with the policies and programs of the Government of Canada.

``...detrimental to the interests of Canada''

Activities ``detrimental to the interests of Canada'' are those which would have a negative impact on the national interests listed in the annual National Requirements for Security Intelligence. When in doubt, the Service should consult with other departments and agencies to determine whether particular activities fall within the meaning of ``detrimental to the interests of Canada.''

``...directed towards or in support of''

Activities ``directed towards or in support of'' espionage, sabotage or acts of serious violence for political purposes are those intended to further, make possible or facilitate espionage, sabotage or serious political violence. There should be a demonstrable connection between such activities and potential acts of espionage, sabotage or serious political violence.

``...relating to Canada''

Acts of serious violence ``relating to Canada'' include those conducted outside of Canada which may put Canada's national interests or Canadians at risk. There should be a direct relationship between activities ``relating to Canada'' and Canada's national interests.

``...clandestine or deceptive''

Activities are ``clandestine'' when an effort is made to conceal them from the Government of Canada or others targeted by such activities, and ``deceptive'' when the activities' origins, motives or objectives are disguised or misleading.

F. Committee Proposal to the Solicitor General of Canada Dated March 18, 1992 about Recommendations in Security Clearance Cases

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

March, 18 1992

The Honourable Doug Lewis, P.C., M.P.
Solicitor General of Canada
13th Floor, Sir Wilfrid Laurier Building
340 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister:

As you know, the Supreme Court recently brought down its decision in the Thomson case.

As you also know, this decision leaves my colleagues and I at the Review Committee in a very difficult position. Well-informed potential complainants in security clearance cases may very well consider it a waste of time and money to appear before us if our recommendations can be simply ignored. This is especially so because our recommendations are made to the very person against whom the complaint is being made.

Evidence of a new attitude among deputy ministers is also at hand. The Chief of the Defence Staff has already withdrawn his appeal to the Federal Court regarding our decision in the Douglas case. He has decided to ignore all of our recommendations in that case, and has written to Ms. Douglas to confirm all aspects of his original decision. The time, money, and emotional cost of her appearance before SIRC has, therefore, been a complete waste as far as she is concerned.

My colleagues and I are most concerned at this turn of events, and we have decided, therefore, to make a proposal to you in an attempt to remedy the damage that has been done to the authority, credibility and effectiveness of this Committee.

Our proposal is attached. I hope that you will consider it at your earliest convenience. It would be most welcome if you could make an announcement outlining a Government policy along the lines we suggest in the near future. In the meantime, it would be a great help if you were to indicate to the House during your statement on March 19, 1992, that the Government is actively considering regulatory changes that would restore the viability of the complaints process.

Yours sincerely,

John W.H. Bassett, P.C., O.C., O. Ont.
Chairman

Attachment

March 18, 1992

SECURITY INTELLIGENCE REVIEW COMMITTEE

PROPOSAL TO

THE SOLICITOR GENERAL OF CANADA

Introduction

Since 1987 the question of whether the Security Intelligence Review Committee's recommendations in security clearance cases should be followed by deputy ministers has been the subject of litigation before the courts. The fundamental question put before the courts was, essentially, whether the government's ultimate responsibility for the security of the country could be fulfilled while, at the same time, allowing an independent body, SIRC, to have the final decision-making power on whether individuals should be granted security clearances.

The members of SIRC are all members of the Privy Council of Canada. They are, therefore, members of the highest constitutional body in the nation. They are not, however, members of that part of the Privy Council, the Cabinet, which has the power, given to it by Parliament, to govern the country.

It would appear to be a reasonable assumption that any body, composed of Privy Councillors, and authorized by Parliament to investigate any particular question or issue, would have the natural authority to enforce its decisions, unless overruled by the supreme authority in the country, also composed of Privy Councillors, the Cabinet.

It is also a reasonable assumption, that Parliament, in passing the CSIS Act, and in specifying that SIRC should be composed of Privy Councillors, had it in mind to create an effective system of redress for complainants, even though it probably did not intend SIRC to have final decision-making power.

The following paragraphs set out the Security Intelligence Review Committee's position on this important question, in the new circumstances created by the Supreme Court's decision in Thomson.

State of the Law

The *Canadian Security Intelligence Service Act*, S.C. 1984, C.21.s.42 (now R.S.G., 1985, c. C-23) elaborates the mechanism for the review of denials of security clearances for public servants and those contracting directly with the Government.

Section 52 of the Act provides:

> 52...
>
> (2) On completion of an investigation in relation to complaint under section 42, the Review Committee shall provide the Minister, the Director, the deputy head concerned and the complainant with a report containing any recommendations that the Committee considers appropriate, and those findings of the investigation that the Committee considers it fit to report to the complainant.

On Thursday, February 13, 1992, the Supreme Court of Canada rendered its judgment in the case of *Her Majesty The Queen v. Robert Thomson and Security Intelligence Review Committee*. At issue was the question of whether a Deputy Minister is bound to follow the ``recommendations" of the Security Intelligence Review Committee. In a majority decision (6-1), the Court ruled that the term ``recommendation" had to be given its ordinary meaning. The Court concluded that the Committee's recommendation was

> ``... something worthy of acceptance. It serves to ensure the accuracy of the information on which the Deputy Minister makes the decision, and it gives the Deputy Minister a second opinion to consider. It is no more than that."

In her very articulate dissent, Mme Justice L'Heureux-Dubé considered the language used throughout the *CSIS Act*, and the specific provision at issue in the context of the purpose or intent of the legislation as a whole. She concluded that the Committee's recommendations had to be more than suggestive:

> ``A fundamental tenet of natural justice is contradicted if the deputy minister can, following a hearing to which he or she has been a party and without any other reasons that those he or she expressed at the hearings, reverse the decision that resulted from the hearing."

Two messages flow from the majority judgment:

1. Deputy Ministers are *not* bound by the recommendations of SIRC, and if they decide to ignore those recommendations they may do so. SIRC simply submits a second opinion to one of the parties who appear before it, and that party, at the end of the process, has the right to make the final decision, without regard to SIRC's recommendation.
2. Persons who are affected by adverse security clearance decisions now know that SIRC has virtually no power to redress any wrong done them.

Supreme Court Decision

The impact of this decision on public servants or contractors who are denied a security clearance is obviously very serious. A process in which an aggrieved public servant spends the

time and money to appear before a quasi-judicial tribunal in an attempt to reverse the adverse decision of a deputy minister, is worthwhile only if that tribunal's decision can be expected to have considerable weight in the final determination of the question.

The new situation created by the Supreme Court decision has already had an important consequence. The Department of National Defence has now withdrawn its appeal under section 28 of the *Federal Court Act* of a SIRC recommendation. The Deputy Minister, in this case the Chief of the Defence Staff, has now written to the person concerned explaining why he has decided to overrule the recommendations of the Review Committee. The person concerned is, therefore, back in the same position as she was before her expensive and time consuming attempt to reverse the original decision by complaining to SIRC.

Principles at Stake

The Review Committee is perfectly prepared to accept the Court's view that the Government of the day has the final responsibility for the security of the country. It follows that the Government should not be forced to accept the decision of an independent body, such as SIRC, which would put it in a position of risking damage to national security. On the other hand, the Parliament of Canada, in passing the Canadian Security Intelligence Service Act, was clearly attempting to provide effective redress in cases where individuals were the subject of adverse security clearance decisions which were mistaken or not properly supported. Since the Supreme Court judgment in Thomson now leaves such individuals in almost exactly the same position as they were in prior to the passage of the *CSIS Act*, it is clear that some action must be taken to restore a more acceptable balance between the Government's right to ensure the security of the country, and a Canadian citizen's right to fairness in his or her treatment by the Government.

It is, therefore, incumbent upon the Government or Parliament to make another attempt to establish a proper balance between individual liberty and the security of the state which the *CSIS Act* has now clearly failed to do.

A Possible Solution

The Committee still believes that the only fully satisfactory solution must be, eventually, an amendment to the *CSIS Act* which makes clear the legislators' intent on the issue of the Review Committee's role regarding security clearances.

However, in the meantime, a Cabinet Directive would suffice to re-establish a reasonable balance between the power of the State and the rights of the individual.

The Government could issue instructions to all Deputy Ministers that Review Committee recommendations regarding security clearances should be acted upon unless:

(a) the deputy minister believed that the Review Committee's recommendation, if acted upon, would pose a threat to the security of the country; or

(b) the deputy minister received new information, unavailable to the Review Committee, which led him or her to believe that the Review Committee's recommendations should not be acted upon.

In the situation described in (a) above, the deputy minister would have the right to present his or her objections to the Review Committee's recommendation, through his or her minister, to the Cabinet. The Cabinet would then make the final decision.

In the situation described in (b) above, the deputy minister would immediately inform the Review Committee that new information was available and would ask for the case to be reopened on that account. The Review Committee would reopen the case in such a circumstance, and would reconsider its original recommendation.

Such a regime would eliminate the current situation wherein a party to a hearing before a quasi-judicial body sitting to consider a decision taken by that party, has, at the end of the process, the right to decide to ignore any or all of the recommendations of that quasi-judicial body. It would also provide an aggrieved public servant or contractor with a redress procedure which would be much more effective than anything now possible. Finally, since the final decision on the granting or withholding of a security clearance would be, as a last resort, in the hands of the Cabinet, the Government's clear responsibility for the security of the country would not be infringed upon in any way.

Recommendation

The Security Intelligence Review Committee, therefore, recommends that the Solicitor General of Canada approach his colleagues in Cabinet at the earliest possible opportunity with a view to obtaining a Cabinet directive to all deputy ministers and other heads of agencies subordinate to the Federal Government instructing them to act as follows:

(a) as a general rule, the Cabinet expects deputy ministers and heads of agencies to accept any recommendations by the Security Intelligence Review Committee regarding the withholding or granting of security clearances to individuals who require them;

(b) in circumstances where the deputy minister considers that SIRC's recommendation would put national security in jeopardy, he may seek his minister's agreement to put the matter before Cabinet for a final decision; and

(c) where a deputy minister has information which was unavailable to SIRC during its investigation of the matter, the deputy minister will ask SIRC to reopen the investigation so as to consider the new information available and reconsider its original recommendation in the light of that new information.

John W.H. Bassett, P.C., O.C., O. Ont.
Chairman

Extracts From Parliamentary Debates Illustrating The Intent of The Government When the CSIS Act was Before Parliament (January 18, 1984 to June 21, 1984)

> ``We are asking Parliament to provide, for the first time in Canada's history, a legal framework more comprehensive, and more detailed, than that of any other security system in the world. Every other country leaves a large part of their security system wholly within the prerogative of government. With Bill C-9 we have tried to reduce that element to an absolute minimum. This Government believes that such an approach is not only desirable, but essential if we are to maintain the necessary balance between national security and the civil liberties that are fundamental to our society... Both Commissions (Mackenzie en 1969 and McDonald in 1981) concluded that to address effectively threats to Canada's security while protecting Canadian civil liberties, our security service should be split out of the RCMP and become more civilian in nature with a legislated mandate and a new system of control and review of security operations."
>
> Hon. Bob Kaplan, Solicitor General of Canada, Febr. 1984, p. 1271

> ``By exchanging the present mandate, established by a Cabinet directive, and thus subject to amendment by Parliament and by Cabinet, for a legislated mandate that can be changed only by Parliament, we are taking a giant step forward in protecting the rights of Canadians."
>
> Hon. Bob Kaplan, Solicitor General of Canada, Febr. 1984, p.1273.

> ``The Review Committee will investigate complaints against the service and will review the security screening process affecting immigration and government employment, investigating specific cases, if necessary. This opportunity to seek review by citizens who are denied government employment, denied promotion... is something new... It should also be considered a great step forward for civil liberties."
>
> Hon. Bob Kaplan, Solicitor General of Canada, Febr. 1984, p. 1275

Before the Standing Committee on Justice and Legal Affairs, Kaplan commented as follows:

``These are very substantial inroads that the citizen has made into the prerogative of the state, and this legislation presents another great inroad by the citizen into the prerogative of the state."

(April 3, 1984) (Issue 10, p. 31)

``... people who even wrongly think they have been victimized by an adverse security decision will have a recourse. That, I think, will enhance the respect of people in the country for national security concerns by knowing that a lot of the suspicions are invalid."

(April 17, 1984) (Issue 15, p. 6)

``It is a very important reform of our law... I think it is one of the highlights of this legislation" (commenting on s. 42).

(May 31, 1984) (Issue 32, p. 40)

G. Solicitor General's Letter of August 19, 1992 About Committee Recommendations in Security Clearance Cases, and Chairman's Reply of August 20, 1992

Solicitor General of Canada

Solliciteur général du Canada

August 19, 1992

The Honourable John W.H. Bassett, P.C., O.C. O. Ont.
Chairman
Security Intelligence Review Committee
14th Floor, Journal Tower South
365 Laurier Avenue West
Ottawa, Ontario
K1P 5W5

Dear Mr. Bassett:

I am writing in response to your letter of March 18, 1992, concerning the Supreme Court's decision in the Thomson case and your proposal on the complaints process.

Following a careful review of the Supreme Court's decision, I do not feel that the Court's decision means Review Committee recommendations ``can be simply ignored.'' In fact, the judgement reinforces the tenet that SIRC plays an important role in the process, that its recommendations must be accorded careful consideration, and that an appropriate balance has been struck between the security of the nation and the rights of individuals.

I can assure you that the Government continues to believe strongly in the importance of the Security Intelligence Review Committee. Deputy heads have placed, and will continue to place, great weight on the recommendations of SIRC in any security clearance case.

At issue in the Supreme Court case was whether a deputy head had to follow the ``recommendation'' of the SIRC in a security clearance case. The Supreme Court confirmed that ``it is reasonable and appropriate that the final decision as to security clearance is left to the deputy minister'' in light of the deputy head's responsibility for security within the department or agency. The Court also noted that the Deputy Minister of Agriculture had considered the SIRC report in making his final security clearance decision regarding Mr. Thomson and supported that decision.

You have indicated that you perceive a change in attitude among deputy heads following the Supreme Court decision. You cited, in particular, a decision by General de Chastelain with respect to Michelle Douglas. Let me assure you, there has been no change in attitude. General de Chastelain made his disagreement with SIRC's recommendation clear from the outset. Following the Supreme Court decision he carefully reviewed the case and concluded that his original decision remained the correct one.

You have also recommended that, in light of the Thomson decision, where a deputy head disagrees with SIRC's recommendation, the matter should be referred to Cabinet for final arbitration. While I cannot agree with this proposal, it may be possible to provide some additional consideration of a case in the event of a disagreement between SIRC and a deputy head, while abiding with the Supreme Court's decision.

The Supreme Court made it clear that the deputy head, as the person responsible for departmental security, must make the final clearance decision. This is in keeping with the deputy head's responsibilities under the *Financial Administration Act*, the *Public Service Employment Act* and ``Security Policy for the Government of Canada'' issued under the authority of the Treasury Board. The latter clearly sets out the accountability of deputy heads for the security function and its administration. It stipulates that a security clearance may only be denied, revoked, suspended or downgraded by a deputy head. When such action might result in release or dismissal, deputy heads are required to consult with the Privy Council Office. In the case of a public servant, dismissal must be approved by the Governor in Council. Referral to Cabinet is not required for members of the Canadian Forces, or for applicants for military or other Public Service positions.

In view of the Supreme Court ruling, the Deputy Head will continue to have the authority and responsibility for the final decision on granting a security clearance. I will nevertheless recommend to the President of the Treasury Board that he consider amending the security policy guidelines to require deputy heads to advise, and consult with the Associate Secretary to the Cabinet and Deputy Clerk of the Privy Council should they disagree with a SIRC recommendation on a security clearance. It is also agreed that after this consultation, the Deputy Head will write to the Chairperson of the SIRC communicating his or her final decision.

In addition, Section 52 of the *Canadian Security Intelligence Service Act* provides that on completion of an investigation, the Review Committee shall provide the Solicitor General and the deputy head concerned with a report. I will continue to use these reports to monitor the process closely.

I hope that this proposal will meet some of your concerns. Our intention remains to ensure that the SIRC is seen as an effective and essential body, whose recommendations are always accorded due consideration.

Yours truly,

Hon. Doug Lewis, P.C., Q.C., M.P.

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

Office of the Chairman

Bureau du président

August 20, 1992

The Hon. Doug Lewis, P.C., Q.C., M.P.
Solicitor General of Canada
340 Laurier Avenue West
13th Floor
Ottawa, Ontario
K1A 0P8

My Dear Minister:

Thank you very much for your letter of August 19, 1992, and, of course, I am pleased to receive your assurances that the important role of the Security Intelligence Review Committee is fully appreciated by the Government of Canada.

I note that you have undertaken to recommend to the President of the Treasury Board that any Deputy Minister overruling a recommendation on a security clearance made by the Security Intelligence Review Committee will be first discussed with the Associate Secretary to the Cabinet and Deputy Clerk of the Privy Council.

I shall look forward to hearing from you when your recommendation is approved and I would appreciate if this could be done as soon as conveniently possible as we are in the process of finalizing our Annual Report which will deal with this matter.

I am also pleased to note that if a Deputy Minister disagrees with a recommendation of the Committee that he will write to the Chairman of the Security Intelligence Review Committee and presumably such a letter will outline his reasons for disagreement.

I am aware of the strenuous efforts of members of your staff in working with Deputy Ministers and staff of the Privy Council office to reach an agreement on future policy that would lessen the concern of the Security Intelligence Review Committee that the Thomson decision would weaken the Committee's ability to protect the rights of individual Canadians.

With kind personal regards.

Yours sincerely,

John Bassett

H. SIRC Staff Directory

The following is a directory of the SIRC staff as of September 15, 1992, when this report went to the printers.

Maurice Archdeacon, Executive Director . . . . . (613) 990-6839
Pierrette Chénier, Secretary 990-8442

Maurice M. Klein, Director of Research
(Counter-Terrorism). 990-8445
Luc Beaudry, Research Officer 990-8051
Joan Keane, Research Officer 990-8443

John M. Smith, Director of Research
(Counter-Intelligence) 991-9111
Michel Paquet, Research Officer 990-9244
Julie Spallin, Research Officer 991-9112

Sylvia MacKenzie, Senior Complaints Officer 993-4263

Claire Malone, Executive Assistant 990-6319

Madeleine DeCarufel, Administration Officer & Registrar 990-8052
John Caron, Records Officer 990-6838
Roger MacDow, Records Clerk 998-5258
Diane Roussel, Secretary 990-8441