



**SECURITY INTELLIGENCE
REVIEW COMMITTEE**

SIRC Annual Report 1998-1999

**An Operational Audit of the
Canadian Security Intelligence Service**

Canada

Security Intelligence Review Committee
122 Bank Street
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

Web Site: <http://www.sirc-csars.gc.ca>

Collect calls are accepted, and the switchboard is open
from 8:00 a.m. to 5:30 p.m. Eastern Standard Time.

© Minister of Supply and Services Canada 1999

Cat. No. JS71-1/1999

ISBN 0-662-64418-2

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

30 September 1999

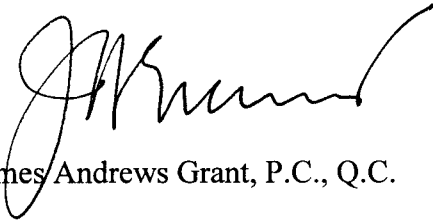
Dear Mr. MacCaulay:

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 1998-99, for your submission to Parliament.

Yours sincerely,



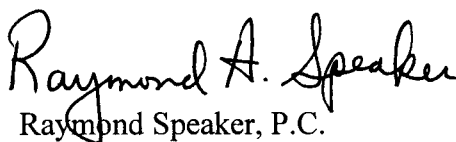
Paule Gauthier, P.C., O.C., Q.C.
Chair



James Andrews Grant, P.C., Q.C.



Robert Keith Rae, P.C., Q.C.



Raymond Speaker, P.C.



Frank McKenna, P.C.

Statement from the Committee

Canada's Security Intelligence System – Life at Fifteen

In strictly legal terms, the Security Intelligence Review Committee (SIRC) was born in July 1984 when the legislation creating it took effect. However, its true genesis was in the tumultuous political and social events of the late 1960s and 1970s which gave rise to a Commission of Inquiry headed by Justice D.C. McDonald, and a report with the deceptively innocuous title, “Commission of Inquiry Concerning Certain Activities of the RCMP.”

Justice McDonald subjected the country's security intelligence apparatus to almost four years of intense scrutiny and he found it wanting. By the time the Commission had finished its work in 1981, Canadians knew two important things most did not know before: that the Royal Canadian Mounted Police in its security intelligence function had routinely committed improprieties and illegal acts against Canadians, and that the security intelligence system of the day was so flawed that it needed to be rebuilt essentially from scratch.

The RCMP Security Service should be disbanded, McDonald concluded, and a new separate, civilian organization put in its place to ensure that security intelligence activities were effective, and at the same time carried out in accordance with the rule of law and accountable to government. After much spirited public discussion the

legislation to create the new agency (the Canadian Security Intelligence Service) and the mechanisms for monitoring its activities (this Committee chief among them) was enacted in 1984.

In a Turbulent World, 15 Years Is a Long Time

Fifteen years is sufficient time to draw some fairly reliable conclusions about the 1984 “revolution” in Canadian security intelligence affairs. At the outset it is important to state that in meeting the goals set by Justice McDonald to create an agency able to “perform effectively in a lawful and proper manner,” the *CSIS Act* and its associated legislative reforms have proven to be remarkably successful. CSIS does its job of identifying threats to Canada and advising the Government about them; SIRC and other responsible bodies including the Inspector General and the relevant committees of Parliament, review the Service's work to help ensure it is effective and that it conforms to the law.

The Members of this Committee would be remiss, however, if we failed to examine and comment on the larger picture beyond our day-to-day reviews of the Service's activities; in this, our view is less sanguine. The plain fact is that some twenty years after Justice McDonald laid out the broad principles for Canada's security intelligence

Justice McDonald subjected the country's security intelligence apparatus to almost four years of intense scrutiny and he found it wanting.

Canadians decided twenty years ago that they would not tolerate a security intelligence agency that did not act within the law.

system there is a growing incongruity between the world for which the existing set of laws and practices were designed almost two decades ago, and the world as it is in 1999.

It is useful to recall that the legislation governing security intelligence in Canada emerged at the height of the Cold War and the depths of the 1980s recession. In 1984 a person by the name of Konstantin Ustinovich Chernenko was head of the Soviet Communist Party, Vaclav Havel had just been released from the first of two terms in a Czechoslovak prison, and few people could tell you what Chechnya was let alone find it on a map.

This is not to suggest that the obvious changes in the world require wholesale revamping of the legislative and administrative apparatus. Indeed, the *CSIS Act* has proved to be quite a flexible instrument for managing intelligence activities in rapidly evolving circumstances. Nevertheless, the number of areas where current policy is either inadequate to the task or altogether silent is significant.

Who's Minding the Store?

Two areas loom as especially problematic. The first concerns security intelligence activities of the Government not covered in existing legislation. The best known is the Communications Security Establishment (CSE). An agency of the Department of National Defence, CSE provides government with foreign signals intelligence in support of Canadian foreign and defence policies. In 1996, the Government for the first time appointed a commissioner to review CSE activities for compliance with the law, and every indication is that Commissioner Claude Bisson is doing commendable work.

Nevertheless, his position is not mandated by any legislation and the office exists at the discretion of the government of the day under the direction of the Minister of National Defence.

Security intelligence activities are on the increase in other parts of the government, in large measure because of the evolving nature of international threats to Canadians. The Departments of Foreign Affairs and International Trade, National Defence, and Citizenship and Immigration Canada are the most active, though there are others as well. None of them, however, are subject to the kind of regulation, direction, and review which currently governs CSIS operations; a state of affairs we believe is not sustainable over the long term.

A key implication of the McDonald Commission's work was that it linked the effectiveness of security intelligence to public accountability. Canadians decided twenty years ago that they would not tolerate a security intelligence agency, irrespective of its goals or achievements, that did not act within the law and in accordance with widely accepted principles of democracy and governmental responsibility. Public confidence that this continues to be the case can only be undermined if it becomes apparent that certain parts of the increasingly varied ensemble of activities called "security intelligence" are arbitrarily subject to less stringent review—or no review at all—than others. In this regard, the recently published report of the Senate Special Committee on Security and Intelligence chaired by Senator William Kelly is an important contribution.¹

Setting National Priorities for Security Intelligence

The second major impact of the sea change in international affairs is the greatly increased threat posed by transnational crime and economic espionage. The Service and other parts of government are responding to these threats and directing increasing resources to counter them. However, a significant challenge to responsible control and review of these activities lies in the current rather oblique language used to describe the threats and decide which parts of government are to deal with them.

The Committee has in the recent past noted instances where the Service has drawn the definition of “economic security” far too broadly for certain activities to be legitimately included within its existing mandate. And as we note in this year’s report, an effective division of labour between CSIS and the RCMP with respect to threats from transnational crime has yet to be realized.

Future effectiveness in dealing with new threats, as well as the capacity to ensure that intelligence activities directed at them are lawful and appropriate, rests in large measure on how the current ambiguities are resolved.

A Comprehensive Review

Canada’s history in the field of security intelligence (not to mention sound public policy making) teaches us that it is foresight and opportunity, not crisis and scandal, which should be the spurs to building upon the achievements of recent years.

The current security intelligence apparatus was designed twenty years ago, and last

examined as a whole in 1990. The Members of SIRC believe that it is time for a thorough Government-wide review of all of the nation’s intelligence systems and organizations. The mechanisms of such a comprehensive examination are for Government to choose, however, we would urge that the review be as open as law and prudence permit, and that all interested parties, individuals, and groups, be encouraged to participate. This Committee would welcome the opportunity to work within any processes that might be undertaken, including any of the appropriate committees of Parliament.

In any democratic society security intelligence activities are among the most serious a government can undertake. They warrant the constant and meticulous attention of all who cherish democratic values and civil discourse in a turbulent and dangerous world.

It is time for a thorough Government-wide review of all of the nation’s intelligence systems and organizations.

How SIRC's Annual Audit Report is Organized

This year's audit report maintains the organization and format instituted in 1996-97. Comments and feedback Committee Members and staff received during the year seemed to bear out our hope that the revised format would be both more functional and more informative.

In general, the report is organized to reflect the Committee's primary functions: first, to review CSIS intelligence activities, second, to investigate complaints about CSIS and associated matters, and third, to act in concert with other parts of the governance system to protect Canadians from threats to their security.

- Section 1 presents the Committee's review and audit of what the Service does and how it does it. The sub-sections represent the different methods the Committee employs to make these assessments.
- Section 2 deals with the Committee's role as a quasi-judicial tribunal with the power to investigate complaints of various kinds.
- Section 3 brings together under one heading—CSIS Accountability Structure—the Committee's review of the multiple administrative and legal mechanisms that hold the Service accountable to Government, Parliament, and the people of Canada.

As before, the report draws a clear distinction between Committee comments, observations and recommendations bearing directly on our major task—reviewing CSIS and associated activities for a certain period of time—and the more general background material we are making available with the aim of assisting Canadians and other readers to understand the context in which security and intelligence work is carried on.

Subjects the Committee believes will be of historical, background or technical interest to readers are set apart from the main text in shaded insets. Unlike the main body of the report, they do not reflect Committee opinion or conclusions as such and are intended to be factual in nature.

A minor but, we believe, important innovation is that where appropriate, each section of the audit report is labelled with the SIRC study from which it is abstracted. The full references are found in Appendix B.

Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1998-99

As has been the practice in recent Annual Reports, the results of special inquiries and concentrated research carried out by the Committee in the course of the year begin our report. These special studies are an addition to and are intended to reinforce the other forms of audit research the Committee undertakes.

Review of Transnational Criminal Activity

Report #107

Organized criminal groups have long been a concern of many democratic governments because of their capacity to disrupt and destabilize the economic well-being of the countries in which they operate, and the threat they pose to law and order. In recent years, criminal organizations both old and new have taken advantage of the greatly increased mobility of populations and advances in communications technology, to extend their activities internationally. In the decade since the end of the Cold War, the activities of the criminal groups emerging from the nations of the old Soviet empire have been of particular concern.

The seriousness of this growing phenomenon was recognized in 1995 when the G-7 states formally recognized international organized

criminal activity as a threat to their security. Many more nations have since strengthened their enforcement efforts, and when they can, have turned to available national security and intelligence resources to assist police in combating the threat.

The Origin of the Service's Interest in Transnational Crime

Following a 1993 Department of Justice legal opinion which embraced the view that transnational criminal activity in certain of its forms could represent a threat to the security of Canada, a role was identified within the Service's mandate whereby CSIS could assist domestic police authorities.² This new CSIS role represented a significant departure from the Service's traditional area of responsibility in which criminal activities were generally investigated only in the context of espionage and serious politically-motivated violence.

Commencing in 1995, the Service initiated a number of investigations into transnational criminal activity using targeting authorities which named individuals, and generic approvals where individuals were not named.³ From the outset, the Service's role was limited to the collection of strategic intelligence. Involvement in criminal matters of a tactical nature more properly the responsibility of police or other law enforcement agencies was to be avoided. The Service's Regions were provided with a set of key objectives for the investigation of the issue-based target (to be discussed more fully below)—objectives which reflected the strategic thrust of the Service's program.

The Service also identified six conditions under which the activities of transnational

The activities of the criminal groups emerging from the nations of the old Soviet empire have been of particular concern.

It was evident to the Committee that CSIS investigators lacked the training and experience to recognize the types of financial and corporate crimes that were supposed to be the object of concern.

criminal groups could be said to represent a threat to the security of Canada. International crime was a threat to Canada when it impacted upon,

- law and order to the extent of affecting the fabric of Canadian society;
- Canada's economic security through such things as large-scale money laundering;
- government programs such as immigration and refugee processes;
- the government's negotiating position with foreign countries;
- Canada's foreign policy interests; and,
- government institutions through such activities as the corruption of public officials.

The first task CSIS set for itself was to establish a solid data base on all the various manifestations of transnational crime. Investigators were authorized to interview persons who may have held relevant information. The Service also made use of its extensive liaison arrangements, both domestic and foreign, to solicit information on the phenomenon generally, and on individuals suspected of being involved.

The focus on the collection of strategic intelligence was restated by CSIS management in November 1997 with investigators urged to make every effort to avoid areas of investigation which fell below the Service's threshold or which had an imminent probability of developing into an enforcement investigation. The Service also took pains to explain its role to domestic government and police agencies, and also to collaborating security/intelligence agencies overseas. In the latter case, CSIS Security Liaison Officers

were instructed to make it known to their foreign counterparts that despite its own strategic focus, the agency was able to "broker" tactical information on transnational criminal activity between them and Canadian enforcement agencies.

Methodology of the Audit

The Committee's 1997-98 audit report examining the Service's cooperative relationship with the RCMP noted CSIS' new initiatives in the area of transnational crime and we stated our intention to conduct a specific inquiry into the Service's activities. The review, the results of which are presented below, was carried out in order to ensure that CSIS investigative activities in relation to transnational crime were consistent with its mandate under the law, its operational policies, and Ministerial Direction.

In selecting cases for special study, our aim was to encompass the spectrum of Service activities: thus we chose an issue-based investigation, an investigation of a foreign-based criminal group in Canada, and the investigation of an individual with suspected links to a foreign criminal group. SIRC researchers examined all files, reports, memoranda, and other documents relating to the selected cases, as well as all policy decisions and instructions governing transnational criminal activity generally.

Findings of the Committee

Training Relevant to the Specialized Nature of the Crimes Involved

The Committee identified several problems that arose quite early in the Service's program. First, it was evident to the Committee that

CSIS investigators lacked the training and experience to recognize the types of financial and corporate crimes that were supposed to be the object of concern. Sophisticated criminal activities such as money laundering, manipulation of international capital flows, securities fraud, and high-level corruption were new to investigators. The Committee's inquiries showed that some thirty months into the program, Service officers were still complaining about their lack of training and some stated that they did not know how to identify certain forms of criminal activity.

"Strategic" and "Tactical" Investigations—a Threshold That Works?

A second problem stems at least in part from the first: the Committee saw that a number of CSIS investigations and inquiries resulted in the collection, retention, and reporting of information on tactical, street-level criminal activities that were clearly not within the scope of the Service's strategic objectives. We believe this results from the fact that the investigative threshold meant to distinguish strategic from tactical intelligence was never adequately defined.

In our review of CSIS cooperation with the RCMP (contained in the 1997-1998 Annual Report) we stated our belief that the terms *strategic* and *tactical* when used in relation to the investigation of transnational criminal activity, were not defined such that they would serve to identify a particular role for the Service. The potential for this sort of overlap was recognized by the Service itself in late 1997. One CSIS official noted that the Service found it difficult to avoid the collection of tactical information which would normally be the province of the police of jurisdiction.

It continues to be the Committee's view, therefore, that where CSIS is unable to bring a unique perspective to a specific area involving transnational crime, it should leave the matter in the hands of the appropriate law enforcement agencies.

Nature of Cooperation Between CSIS and Overseas Agencies

The Committee's third general concern touches on the Service's international contacts. Its focus on strategic intelligence had an unanticipated impact on relationships with collaborating foreign security and intelligence agencies. CSIS learned over time that these agencies were interested in tactical intelligence on transnational crime in support of law enforcement organizations in their own countries. In spite of the Service's offer to serve as a link to the Canadian agencies concerned, the overseas security and intelligence agencies—working partners with CSIS of long standing—established their own direct links with Canadian law enforcement agencies. The intelligence "brokering" role that CSIS saw for itself did not develop as planned and the Service was to some extent left out of the intelligence information exchange.

CSIS Contribution to Canada's Fight Against International Crime

The Committee's review identified several instances where the collection by the Service of strategic information (and its subsequent dissemination to the appropriate government agencies) played a crucial role in government decision making. In addition, the Service's strategic data base on transnational crime aided Citizenship and Immigration Canada

Where CSIS is unable to bring a unique perspective, it should leave the matter in the hands of the appropriate law enforcement agencies.

The Committee was encouraged to note the increasing flow of information from CSIS to departments and agencies of government having particular responsibilities for foreign trade and economic development.

in preventing the entry into Canada of certain organized crime figures based overseas.

The question arose in an earlier review (See 1997-1998 SIRC Annual Report, page 32) as to whether CSIS was providing the RCMP with all the information it had on transnational criminal activity. During the period reported on here, the Committee found that for the most part all tactical or other criminal information that was collected in the course of its strategic investigations was passed promptly to the RCMP or to the police force having jurisdiction. While SIRC researchers did come across a number of tactically relevant reports that bore no positive indication of being passed to police authorities, it was not possible to determine whether the contents of the reports had been provided to police verbally.

Domestic Liaison Matters Requiring New Policy Direction or Clarification

The existing liaison arrangements between the RCMP and CSIS provide for an exchange of liaison officers at the national and regional headquarters level. By virtue of the RCMP's responsibilities under the *Security Offences Act*, RCMP liaison officers are provided access to all reports that relate to the Service's Counter Terrorism Program originating from the headquarters to which they are attached. However, the Service's transnational crime investigations are conducted not by its Counter Terrorism staff, but rather by its Counter Intelligence officers—whose product is not routinely available to the RCMP in all regions. It is thus left to Service personnel in some regions to assess the incoming transnational crime intelligence and determine its relevance to the RCMP.

It is the Committee's view that the current administrative division of labour holds out the possibility of inadvertent failure to pass on important information to the RCMP. We believe that Service policies should be reviewed to eliminate that possibility.

The Committee was encouraged to note the increasing flow of information from CSIS to departments and agencies of government having particular responsibilities for foreign trade and economic development. The advice provided to these agencies assists them in ensuring that foreign criminal groups do not become involved in, or derive benefit from, Government of Canada programs.

One instance that did raise a note of caution concerned a serious case where a fraud involving several million dollars may have prompted a government agency to seek the Service's help. In the request for assistance there was the implied expectation that in the future, in order to ensure that there were no transnational criminal connections involved in joint ventures with foreign parties, the Service would routinely conduct background checks on companies and individuals seeking the government agency's financial backing.

While there seems to be no reason why adverse information already in the Service's possession should not be provided to the agency, in our opinion there is no legal basis for the Service to initiate such inquiries without there being reasonable grounds to suspect that there is a threat to the security of Canada. It is the Committee's view that a clarification in written policy would help ensure that no inappropriate investigations are undertaken in similar situations.

The “Issue-based” Investigation

The use of generic, or issue-based targeting authorities by the Service, enables it to investigate a class of threat activity, or a particular group or organization, where there are reasonable grounds to suspect that the activities represent a threat to the security of Canada, but where the identities of the individuals involved may not be known.

The generic targeting authority in the case we examined was intended to give CSIS the means to obtain a strategic overview of transnational criminal activities linked to a specific group of countries. It is the Committee’s view that as a general rule, once the identity of an individual becomes known through the use of a generic targeting authority (and there exist reasonable grounds to suspect that the person’s activities represent a threat to the security of Canada) the Service is obligated to obtain a specific targeting authority in order to continue an investigation of that individual. Our review of the general targeting authority came across two instances where investigative activity was continued against known individuals under the generic targeting authority.

In the first case, after establishing the identity of an individual under the generic targeting authority, the Service continued to investigate and collect information on that person. Our review of the documents indicates that there probably were sufficient grounds to suspect the individual of threat activities, in which case a new, specific targeting authorization would have been justified. The Committee believes that the Service’s continued investigation of the individual in the absence of

such authorization may have been an inappropriate use of issue-based targeting.

In the second case, instructions from CSIS Headquarters were sent to a number of regional offices to collect certain information under the generic targeting authority. One office questioned whether the generic authority was sufficient to collect the requested information and was informed that a specific targeting authority would indeed be sought.

This instance raised two issues for the Committee. The fact that the specific authority was obtained only after the original headquarters request was questioned by a regional office indicates that there may be gaps in the articulation and comprehension of the Service’s policy concerning issue-based targeting and transnational criminal activity. We were informed that the CSIS *Operational Policy Manual* includes no such specific policy instructions. The Committee believes these omissions should be rectified. Secondly, the nature of the response by headquarters to the regional office query revealed a perspective on the use of issue-based targeting which was not supportable, in the view of the Committee.

The Specific Investigations

The two specific target authorizations the Committee reviewed were a known foreign criminal organization and an individual with suspected links to it. The activities attributed to the individual included an alleged major fraud against an agency of the Canadian government. Given the extent and complexity of the activities involved,

There may be gaps in the articulation and comprehension of the Service’s policy concerning issue-based targeting and transnational criminal activity.

The question of whether CSIS' mandate permits its involvement in the investigation of transnational criminal activity remains open at the present time.

the Committee believes that a foreign influence case against the individual had yet to be made. Should no clear foreign influence be established, and the suspected criminal activities be on his own behalf, it is our view that any further investigation should be a matter for the police.

Other Countries' Handling of Transnational Criminal Activity

Documents collected by CSIS and read by the Committee during the course of its review provided insight into the way several allied security and intelligence agencies investigated transnational criminal activity. To a large extent, the investigative activities of these foreign agencies were "client-driven"—the client being either the police or a national criminal intelligence organization. With one exception, intelligence agencies concentrated on gathering information intended to be used in direct support of law enforcement measures. CSIS pointed out that it assisted law enforcement as well as other Federal departments and agencies in a similar fashion.

Conclusions and Recommendations

From the Committee's perspective, the question of whether CSIS' mandate permits its involvement in the investigation of transnational criminal activity remains open at the present time. In the coming months, we will present our views on the issue.

The Committee believes that the problems CSIS has encountered in this area can be attributed, at least in part, to the lack of familiarity and experience which naturally accompanies venturing into a new field. In the event that the Service continues to be

involved in this sector, we believe several measures are warranted.

The threshold for CSIS intervention ought to be clearly articulated: Service participation should be contingent on the criminal activity being of such seriousness and scope as to represent a genuine threat to the strategic, social, economic, and national security interests of Canada. The Service should not become involved in the investigation of criminal activities best left to law enforcement agencies.

There is a larger public policy question to be addressed by Government. Currently, CSIS is following Ministerial instructions to deal with issues of international crime. However, our reviews indicate that the Service may not be equipped either by tradition or by training to take on the task. Given the importance of the matter, we would urge the Government to consolidate and clarify its intentions on how to address this growing array of threats to Canada.

Should CSIS continue to remain involved in the area, the Committee recommends that,

it develop a clear operational policy in all its aspects for investigating transnational criminal activity. Such policy should include the requirement to assess each case whenever consideration is given to initiating an investigation under an issue-based targeting authority; and,

it implement a program of special-

ized training in the key areas of transnational crime in order that the objective of providing strategic intelligence to the government on major international criminal activities can be fully realized.

Review of Intelligence Production

Report #110

The Service's primary mandate has two key elements: first, to "collect, analyze and retain information and intelligence" on threats to Canada, and second, to "report to and advise the Government of Canada" on these matters. Within CSIS, Counter Intelligence and Counter Terrorism branches perform the collecting function, while Requirements, Analysis and Production (RAP) Branch has a major, though not exclusive, role in producing reports and advice. The RAP Branch is thus one of the transmitters of information between the gatherers of data and intelligence and the rest of the Service, and between CSIS and the rest of Government. As part of the 1998-99 research program, the Committee undertook to review the activities of the RAP Branch of CSIS.

Methodology of the Audit

Between September and November 1998, SIRC researchers interviewed RAP personnel at all levels to learn about the Branch's structure, its production processes, and the manner in which priorities are set and implemented. We reviewed the advice that the Service provided to Government by examining selected statements from *CSIS*

Reports and Intelligence Briefs prepared by RAP during fiscal year 1997-98, and comparing them with the source material used in their creation. We also interviewed a wide range of RAP's clients outside the Service to determine whether their intelligence requirements were being met.

Previous Studies

Serving as a valuable baseline for this year's review of RAP were two previous studies.⁴ The first was carried out by the Independent Advisory Team (IAT) in 1987 headed by the Honourable Gordon Osbaldeston. The IAT observed in what was then called the Intelligence Assessments Branch (IAB) serious organizational deficiencies that affected the quality of intelligence production. At that time, CSIS research and analysis functions (operational analysis, strategic analysis, and "research") were carried out in three separate directorates. Coordination was difficult and had a negative impact on the Service's ability to produce intelligence that adequately responded to Government needs. Osbaldeston's team recommended an amalgamation of all three components into one functional unit.⁵

The IAT report also highlighted the absence of clearly defined intelligence priorities, the lack of a coordinated system for production, and inadequate reference facilities. Too much emphasis, it said, was placed on the short-term analysis of events as they unfolded, and too little on longer-term analysis that would help the government develop policy and make strategic decisions. Osbaldeston recommended that CSIS develop a strategic plan for intelligence production based on the Government's intelligence priorities, and adopt an inte-

The RAP Branch is thus one of the transmitters of information between the gatherers of data and intelligence and the rest of the Service, and between CSIS and the rest of Government.

CSIS needs to take greater care in distinguishing between “analysis” and statements of fact in its products.

grated approach to the collection, analysis, and dissemination tasks.⁶

The second study was conducted by the Committee one year later. Our in-depth review in 1988 found that the operational branches remained preeminent in the intelligence production process, one result of which was the continued over-emphasis on short-term intelligence to the detriment of strategic analysis. Two key recommendations emerged from the review. We recommended that CSIS management decide whether to continue with the status quo or take the active steps necessary to develop a strategic analysis capacity.⁷ In addition, we suggested that the Intelligence Assessments Branch undertake to recruit outside professionals with experience in strategic intelligence and knowledge of the social and cultural backgrounds of CSIS targets.⁸

RAP Today

In 1992, the Service addressed most of the points raised by the IAT and our own audit in a reorganization of the Intelligence Assessments Branch. Renamed the Requirements, Analysis and Production Branch, RAP created first a Strategic and Emerging Issues Section to conduct strategic analysis and focus on emerging security intelligence issues, and later a Marketing and Client Relations Unit to respond more effectively to the Government’s requirements.

Since the critical restructuring of 1992, there have been additional changes to the way RAP functions. Previously organized along geographic lines, RAP’s structure mirrors more closely that of the other operational

branches in order to eliminate duplication of research and more clearly develop expertise. The Strategic Analysis Unit that provided longer-range analysis to the Government was recently disbanded to allow the integration of strategic analysts into operational areas.

Findings of the Committee

Client Assessment of RAP Products

We examined the quality of reports produced by RAP. Selecting statements from ten branch products not self-evidently supported by the rest of the text, we then examined the documents employed as source material. The overall conclusion we were led to was for both internal and external clients, CSIS needs to take greater care in distinguishing between “analysis” and statements of fact in its products.

We interviewed a number of RAP clients in order to gain insight into consumers’ views of Service intelligence products. Generally the comments were positive: “CSIS Reports are clear, well written, easy to follow, and provide good background information on a series of subjects.” Service reporting to clients was seen to be timely, with specific mention being made of recent CSIS reports on Information Warfare. There was some concern expressed about not knowing when Service intelligence products could be expected to arrive.

On a more critical note, several clients told us that they were often in receipt of RAP products that did not directly address their departments’ operational requirements. Others believed that RAP reports were

sometimes over-classified considering the information they contained, thus limiting their distribution.

Setting Branch Priorities

RAP has been in an almost continuous cycle of change during the last decade in an effort to accommodate the needs of its various clients. Despite these efforts, the influence of the operational branches predominates simply because they are the primary sources of information about threats to national security.

A number of factors led us to this conclusion. The Branch produces an annual plan that is based, in large measure, on the National Requirements that are shared by the operational branches, with the needs of external clients appearing to play little role. In addition, Government clients lack the information from CSIS that would permit informed choices about the intelligence products available. And finally, external clients when meeting with the Service to discuss their needs are told that RAP may or may not act upon a particular request. It is evident that some clients may not fully appreciate the limitations of CSIS mandate and the impact this may have on the Service's ability to act on certain requests.

While the Committee acknowledges the organizational reality that clients in Counter Intelligence and Counter Terrorism will continue to influence much of what RAP does, we remain convinced that the Service should continue its active efforts to accommodate its external partners, and that it is possible to seek a better balance without

penalty to internal operations.

There is a similar lack of balance in the area of strategic analysis. Our discussions with both RAP's internal and external clients evinced the clear need for more and better long-range, strategic analysis.

In order to redress these shortcomings, set balanced production priorities, and avoid a situation where the Government is not as well informed as it should be, renewed direction from CSIS senior management is required. To this end, the Committee has two recommendations:

the reinvigoration of an apparatus that has become defunct in recent years—the Executive Intelligence Production Committee (EXIPC).⁹

the articulation by CSIS of a specific plan to meet the clear requirement of both internal and external clients for more strategic analysis.

Quality Control and Staff Morale

The Committee's review showed that analysts are given little formal training when they join RAP, although the Service has stated it intends to introduce formal training sessions in the near future. There are no written guidelines about how intelligence reports are to be produced, however, earlier Branch products serve as examples and senior analysts act as mentors.

Our review also identified a troubling form of professional segregation within the Branch. RAP staff who are not classified

Some clients may not fully appreciate the limitations of CSIS mandate and the impact this may have on the Service's ability to act on certain requests.

The Service should continue active efforts to accommodate its external partners, ... it is possible to seek a better balance without penalty to internal operations.

as intelligence officers (IOs) are treated differently in the areas of salary, training, and career advancement. Officers in the non-IO categories do not benefit from operational experience or foreign postings, and they are paid significantly less. We learned of the case of one non-IO staff member who after serving in an acting capacity as a manager for two years was then denied the opportunity to compete for the position. The person has since filed a grievance.

In order to address these issues, the Committee recommends,

that the Service develop quality control guidelines and protocols for its written product, and devise methodologies for checking the veracity of information on which reports are based.

that CSIS implement a comprehensive career plan encompassing all RAP officers, IOs and non-IOs alike. Ideally, the new career plan would include more scope for professional growth within the Branch while maintaining opportunities for movement within the Service, and into the larger public service when appropriate.

that a reasonable proportion of supervisory positions within the RAP establishment be designated for officers in the non-IO category.

Activities in Canada

Report #115

For this study the Committee reviewed CSIS investigations of the activities in Canada of a foreign state's intelligence services. We last looked at the Service's investigations in this area a number of years ago, and now as then, the Service's investigations centered on the activities of several members of the country's diplomatic service, posted to missions in Canada and acting as declared and undeclared intelligence officers.¹⁰

Our audit set out to assess the threat (as described in sections 2(a) and 2(b) of the *CSIS Act*) posed by the foreign intelligence services under investigation, to determine whether the Service's investigations were proportionate to the threat, and to verify Service compliance with the provisions of the *CSIS Act*, Ministerial Direction, and CSIS operational policies.

Methodology of the Audit

The Committee's review included the following:

- a warrant affidavit and the supporting documentation, in order to ascertain the basis for the CSIS investigations;
- the Request for Targeting Authorization (RTA) which began the investigative process;
- several investigations, chosen at random, of foreign intelligence officers in Canada;

Review of Foreign Intelligence

- several human source files associated

- with the investigations; and,
- many of the most sensitive files held by Service in order to understand the extent of the operations conducted by the foreign state's intelligence services on Canadian territory.

The Threat

The Committee was satisfied that the documentation did support the conclusion that the intelligence services of the foreign state concerned remained a significant threat to Canada. We examined the resources directed against the threat, and certain measures of the threat itself. While assessments of the threat written by allied governments and made available to the Service contained some contradictory information, the Committee regards the level of resources devoted by the Service to the threat as appropriate.

Based on our review, the Committee agrees that the “reasonable grounds to suspect” that the foreign intelligence officers in Canada were involved in the covert collection of classified or proprietary information were present. However, in certain of the circumstances we reviewed, the threat did not appear to be particularly pressing or significant. Nevertheless, we also saw compelling and irrefutable evidence that this foreign government continued to direct significant clandestine intelligence activities against Canada.

We noted CSIS' assertion that the intelligence services under investigation were increasingly employing non-traditional techniques so as to minimize the risk of diplomatic “spy scandals”

should their operations be uncovered. While the Committee believes that the use of non-traditional forms of “cover” represent a potential threat, our review of the base documentation led us to believe that this form of threat had not been established to the extent suggested by the Service.

Findings of the Committee

While we were able to draw conclusions about the overall, long-term threat to Canadian security posed by the foreign state's intelligence services, the level of threat in individual cases was less apparent. Intelligence operations are inherently protracted affairs; when coupled with the limited time frame (one year) covered by our review, definitive conclusions about the threats posed by individual targets are difficult to draw. We were, however, able to fully evaluate the conduct of the Service's investigations in relation to compliance with operational policy, procedures, Ministerial Direction, and the *CSIS Act*.

Retention of Information

The Committee identified one item of information in the Service's data base that did not meet the “strictly necessary” test for collection and retention. The information, in our view, was incidental to the investigation and unrelated to the activities of the targeted foreign intelligence services. We have so informed the Service.

Fact in a Request for Approval

In the course of reviewing base documents for a Service operation that extended over a number of years, we found an error of fact in a request for approval sent to the Solicitor

We saw compelling and irrefutable evidence that this foreign government continued to direct significant clandestine intelligence activities against Canada.

It is not unusual for persons (including Canadians and Canadian residents) in contact with known or suspected intelligence officers to be approached by the Service for information.

General. The request was to approve an operation and incorrectly identified the country where similar types of the operation had been successful. The correct information had been available to CSIS staff at the time of the request. We brought this to the attention of CSIS and it agreed with our assessment.

Policy in the Case of a Sensitive Operation

The Committee examined an operation against an intelligence officer posted to Canada. The officer had sought information about Government policy. As a result of our examination of the case, we concluded that a Government department should have been given certain information about the matter. Service files showed that this had not occurred. We advised the Service of our findings.

CSIS Contacts with Canadians During Counter Intelligence Operations

The CSIS investigations we examined were all directed at foreign nationals, however, it is not unusual for persons (including Canadians and Canadian residents) in contact with known or suspected intelligence officers to be approached by the Service for information. In one case we came across during our review, we noted the considerable efforts by the Service to explain to an individual contacted for such purpose that he was not the subject of investigation.

CSIS Investigations on

University Campuses

Report #114

Security intelligence policy in Canada treats university campuses as “sensitive institutions.” Investigations associated with any university, technical institute, community college or CEGEP are thus subject to policies and procedures more stringent than most other areas of Service investigation. The purpose of this study was to examine the use and effectiveness during the audit period of these additional procedures—specifically, the Ministerial Direction authorized in 1997—and to review CSIS investigative activities at post-secondary institutions for compliance with Ministerial Direction, the *CSIS Operational Policy Manual (OPS)*, the *CSIS Act*, and other relevant legislation.

Methodology of the Audit

The review covered the period 1 March 1997 to 30 September 1998 and involved examination of a broad range of Service files and documentation (both electronic and hard copy):

- Aide-mémoire on campus operations approved by the Minister; and the authorizations by the Minister, the Director of CSIS, and senior managers.
- Human Source Branch correspondence concerning policy on investigations at post-secondary institutions.
- Authorizations for investigations approved by senior CSIS managers pertaining to post-secondary institutions.
- Human Source Branch administrative

files, and source handler reports.

- section 12 data base reports about any targets of CSIS investigations who were staff, students, or employees at the post-secondary institutions.

History of Campus Investigations Policy and Practice

1963 Agreement with CAUT

Existing campus investigation policy has its origin in a 1963 agreement between the Federal Government and the Canadian Association of University Teachers (CAUT). Known as the Pearson-Laskin Accord, the agreement was a policy response to concerns about RCMP Security Service campus investigations during the 1950s and 1960s. The agreement articulated policy affirming that the Security Service would enter onto post-secondary institutions only to conduct security screening or “where there [were] definite indications that individuals may be involved in espionage or subversive activities.”

The Accord noted specifically that,

no informers or listening devices will be used on university campuses except where the Solicitor General has cause to believe that something specific is happening beyond the free flow of ideas on university campuses.

The basic message of the Accord appears to be that the Government would not engage in general surveillance of universities and colleges. The Accord contained the specific statement, “there is at present no general

RCMP surveillance of university campuses.”

Subsequent policies dealing with campus investigations have carried forward the principles of the 1963 agreement. They were restated in 1971 in the form of a Cabinet record, and again in 1984 when just prior to the passage of the *CSIS Act*, the Solicitor General published the Ministerial Direction, “Security Investigations on University Campuses.”

Following closely the wording of the 1963 Accord, the Ministerial Direction states that security investigations on campus were only to take place where there were “definite indications that individuals may be involved in activities prejudicial to the security of Canada.” The essence of the Direction was that the Minister had to approve the use of human sources and other intrusive methods on campus.

Application of the 1984 Ministerial Direction

By the mid-1990s it was apparent that in its application, the 1984 Ministerial Direction was flawed. Because it predated the *CSIS Act*, it employed tests, procedures, and legal terminology not found in the *CSIS Act* — the founding legislation for the new Service that had to use it.

There were also operational problems created by the need for the Service to seek Ministerial approval to investigate any and all campus activities no matter how far removed they were from the “free flow of ideas” in the academic milieu. This gave rise to an authorizing procedure not in

Security investigations on campus were only to take place where there were “definite indications that individuals may be involved in activities prejudicial to the security of Canada.”

Lawful Advocacy, Protest, Dissent, and Sensitive Institutions

Sensitive operations invariably involve the use and direction of human sources, and while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on societal institutions, legitimate dissent, and individual privacy.

The *CSIS Act* specifically prohibits the Service from investigating “lawful advocacy, protest or dissent” unless carried on in conjunction with threats to the security of Canada as defined in the *Act*. The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions, and university campuses.

keeping with the principles of the 1963 accord. The Service disagreed and noted that successive Solicitors General have provided CSIS with the authority in question.

Both the Review Committee (in 1991) and the Inspector General (in 1995) found the policy wanting, and so stated.

Policy Revision of 1997

In 1997, the Solicitor General issued new Ministerial Direction—“Security Investigations at Post-Secondary Educational Institutions”—meant to address the problems and bring policy in line with existing legislation. The general principles of the 1963 agreement were retained, and investigations had to be consistent with the tests of the *CSIS Act*, particularly in its protection of lawful advocacy, protest, and dissent.

The 1997 Direction made two fundamental changes. The Director of CSIS was delegated the authority to approve source activities which while located on campus were entirely removed from the academic milieu. The

Director was to provide the Minister annually with a “summary” of all such cases approved.

In addition, the Director was also delegated the authority to employ sources on campus in situations where there was no possibility of obtaining the prior approval of the Solicitor General. The Director was obligated to notify the Minister as soon as possible thereafter about the circumstances of the operation.

Like its predecessor, the new Ministerial Direction recognized the need for CSIS officers to visit campuses to conduct security screening investigations, but cautioned that these were not to be used as a pretext for other investigations.

Findings of the Committee

Consistency in Articulation of Policy

As a general rule, CSIS officers rely on relevant sections of the *CSIS Operational Policy Manual* which are derived from Ministerial Direction. Therefore, an examination of the Service’s interpretation of

Ministerial Directions, as expressed in its policy manual, was an important part of our review. The Committee identified some potential problems:

- in instances where the Minister's approval is still needed, the policy manual excluded the requirement set out in Ministerial Direction that the Service provide an explanation to the Minister of how the proposed operation would affect the rights and freedoms of the subjects of the investigation and others associated with the institution;
- a term for a particular type of investigative activity has been subject to too broad and varied an interpretation;
- the policy contained no references to the seminal 1963 Pearson-Laskin Accord; and,
- the policy permits CSIS officers, without Ministerial approval, to go on campus to collect information for security screening purposes and for other mandated enquiries; the purpose and scope of such enquiries not being adequately defined.

Campus Investigations and Operations

During the eighteen-month period covered by the audit, there were two cases where CSIS employed its newly delegated authority. In the first, the Director of CSIS approved a procedure for the continuation of an activity that had been agreed to by the Minister the year before. The Director's decision was based on staff advice that the investigative activity would not affect the free flow of ideas and normal academic life at the institution and was thus permitted under

Ministerial Direction.

The Committee questioned whether the one-year approval for the procedure was in keeping with the essence of the 1963 Accord. CSIS asserted that the authority was consistent with post-1963 legislation, Ministerial Direction, and Service policies.

We noted too that Ministerial Direction dictates that the Director report by way of summary to the Minister following operations where approval had been delegated to the Director. Apart from a one-line reference in the Director's Annual Report, the Committee could locate no other document that would indicate that the Minister had been informed of the matter—in the Committee's view, less than adequate compliance with Ministerial Direction.

In the second case where the 1997 Ministerial Direction had delegated authority to the Director, CSIS provided information that substantiated his decision. However, the Committee subsequently learned that the Service did not comply with the requirement to immediately inform the Minister afterwards. When the Minister was eventually informed about the operation—some eight months after the event—CSIS gave the reasons for the administrative error and informed the Office of the Inspector General.

One Minister-approved operation which occurred during the audit period was a cause for concern. The investigation involved the activities of a foreign power and persons working specifically on its

The Service should be required to explain how a particular investigation will impact on the rights and freedoms of persons who are subjects of the investigation as well as those persons associated with the institution concerned.

The Service collected and retained information that extended beyond the original targeting authority.

behalf in Canada. While the preponderance of the targeting and reporting was entirely legitimate, our review showed that the Service collected and retained information that extended beyond the original targeting authority. It is the Committee's view that the reporting was unwarranted and not in accord with current policy or the principles which have governed investigations at post-secondary institutions since 1963.

Conclusions and Recommendations

Two recommendations emerged from our study of CSIS campus operations:

First, when requesting authorization from the Minister, the Service should be required to explain how a particular investigation will impact on the rights and freedoms of persons who are subjects of the investigation as well as those persons associated with the institution concerned.

The Service has acknowledged this lacuna and has stated that it will prepare new policy to address the issue.

Second, the CSIS policy manual should include in the authorities section explicit reference to the 1971 Record of Cabinet Decision articulating the general principles of the Pearson-Laskin Accord on campus investigations.

CSIS saw no need for this in view of the changes after 1963 to legislation, Ministerial Direction, and Service policies.

CSIS Cooperation with the

RCMP - Part II

Report #108

Among the most important of the Committee's responsibilities is the requirement to examine all agreements concluded by CSIS with other agencies and to monitor any exchange of information and intelligence they might entail. It is with respect to this part of the Committee's mandate that we present the results of the second of a two-part inquiry into relations between the Service and the RCMP.

Concentrating on the cooperative relationship at the headquarters level, Part I of the study was included in SIRC's 1997-1998 annual audit. Our goal in that review was to identify systemic problems in the relationship that would impact on the ability of either agency to fulfill the responsibilities assigned to it in the relevant governing legislation and in the principal instrument where the nature of the cooperative arrangement is articulated—the Memorandum of Understanding.

In Part I, the Committee identified several problem areas which we believed had the potential to adversely impact on the Service's effectiveness. We stated at the time, however, that a well-grounded assessment as to their significance and seriousness could not be made without examining the operational relationship in some detail. Part II, therefore, was directed principally at contacts and cooperation between the Service's regional offices and the corresponding RCMP geographical divisions.

Our specific purpose was to evaluate how

well the CSIS-RCMP arrangement was working at the regional and operational level, determine the extent to which problems identified earlier represented a potential impairment to the operations of either agency, and, if possible, suggest ways to correct or minimize them.

Methodology of the Audit

After reviewing selected files and data provided by the six regional offices of CSIS, including records of information exchanges with their counterpart RCMP divisions over the period June 1997 through March 1998, we selected three CSIS regional offices for further study.

In addition to examining all files and other documentation (hard copy and electronic) relevant to exchanges of information between the two agencies, SIRC researchers conducted extensive interviews with representatives of the Service and the RCMP. The opinions and judgements reflected in these interviews were of considerable importance in helping the Committee gain a proper understanding of the RCMP-CSIS relationship. Also necessary for this deeper understanding was consideration of events before and after the formal review period.

Findings of the Committee

Protection of Sources vs. Criminal Prosecution: an Enduring Dilemma

The mainstay of the operational relationship between the two agencies is the exchange of information via liaison officers in CSIS regions and RCMP divisions. While this part of the information exchange mechanism appeared to be working well in achieving

its basic goal—providing each side initial access to key information and intelligence produced by the other body—the effective use of the information in certain situations appears to some within the RCMP to be more problematic.

Among the RCMP officials we interviewed there was a general sense of dissatisfaction about the restrictions imposed by the Service on the disclosure and subsequent use by the RCMP of CSIS-generated information and intelligence. Most seemed to realize, however, that the restrictions flowed from the legal requirements for discovery and disclosure inherent in criminal proceedings and, in particular, the *Stinchcombe* decision.

As discussed in Part I of the study, some tension between the two agencies over the handling of CSIS-generated information is inevitable given the differing requirements and mandates of the two agencies. The Service exists to collect intelligence on threats to Canada using sources and methods that must be protected if they are to continue to be effective. On the other hand, the RCMP is an enforcement agency which like the Crown prosecutor, is obligated to disclose information to the Courts in support of formal judicial proceedings. In short, the Service is content to provide sensitive intelligence to the RCMP on the condition it does not reveal the information or its source. At the same time, the RCMP may need to disclose the nature of the information if it is to effectively pursue criminal prosecution and in some situations can be legally compelled to do so.

As we had anticipated upon the conclusion

Some tension between the two agencies over the handling of CSIS-generated information is inevitable given the differing requirements and mandates of the two agencies.

R. v. Stinchcombe 1991 3 S.C.R. 326.

The Stinchcombe case involved a criminal proceeding where the Crown had interviewed a witness who had given evidence earlier in the proceeding that was favorable to the accused. The Crown concluded that the evidence of this witness was undependable and decided not to call the witness in the trial. The defence sought disclosure of the interview in the belief that it might contain information favorable to its case. The Crown refused. The case went to the Supreme Court, which ruled in favour of a general duty of disclosure (other than for irrelevant information or information which was privileged) on the Crown (but not on the defence). Essentially the reasons for this ruling were:

1. Disclosure eliminates surprise at trial and thus better ensures that justice is done in a proceeding.
2. The duty of the Crown in a criminal proceeding is to lay before a trier of fact all available legal evidence: it is there to secure justice, not simply a conviction. Thus, the fruits of the Crown's investigation are the property of the public to be used to ensure that justice is done. (Defence Counsel, on the other hand, is there to defend the client's interests to the extent permitted by law.)

Stinchcombe, as such, did not deal with administrative law. The Court was careful to specify that in reaching its conclusions it was not to be taken as laying down principles for disclosure in circumstances other than criminal proceedings by indictment. For this reason, the Court did not look beyond the criminal law setting in its analysis. Notwithstanding the Court's express attempt to limit the impact of its ruling and notwithstanding the criminal nature of the proceedings, the decision has been extended to administrative proceedings. Numerous cases have emerged inspired by the principles enunciated in Stinchcombe.

of Part I of our inquiry, this ongoing dilemma has resulted in a number of localized difficulties that are the cause of some concern. In the opinion of some officers at one location, RCMP requests for the disclosure of CSIS information had declined significantly because successful prosecution could have been imperilled by legal challenges involved with using CSIS information. In the Committee's view, such an attitude to requests for disclosure cannot fail to have a detrimental effect on the operations of both agencies. The RCMP has assured us, however, that nationally the number of requests for disclosure has been relatively constant. There is no obvious solution to this conun-

drum within the existing Memorandum of Understanding or under existing legislation. While the potential impact of changing the law is open to debate, what is not in doubt in our opinion is the potential for damage to national security operations should the situation be left unchanged.

RCMP Liaison Officers and Alternative Information Channels

Our audit of the cooperative relationship at the regional level revealed problems in the manner in which CSIS information is provided to the RCMP. The records of exchanges show that a considerable volume of information is provided directly to functional commands

in the RCMP. The effect is to leave some RCMP liaison officers with an incomplete picture of what has or has not been provided. While the nature of RCMP arrangements to handle and process incoming information is outside the Committee's mandate, we believe that the current system could negatively influence future cooperation with the Service. We are also aware that the RCMP is seized with the problem and is studying appropriate solutions.

Overlap of Responsibilities at International Airports

The Federal Government recently transferred jurisdiction for policing at Canada's international airports from the RCMP to local police forces. A Federal policing presence was to remain, however, through the creation of RCMP Airport detachments drawn from the National Security Investigation Section (NSIS), a branch of the Force responsible for the investigation of activities described in the *Security Offences Act*.

At the outset of our inquiry there appeared to be the potential for overlap between this new organization and that of the Service which also has a presence at ports of entry—mainly in the role of assisting Citizenship and Immigration Canada in immigration security screening. (See page 9 of the 1997-98 SIRC Annual Report for a description of CSIS role in immigration.) While we found that the presence of the RCMP units at the airports created some initial confusion among other enforcement agencies as to respective mandates and responsibilities, these were quickly dispelled and have resulted in no serious difficulties.

Transnational Criminal Activity

Commencing in 1996, the Service undertook to investigate transnational criminal activity on the basis that the huge financial resources generated by international money-laundering and other illegal enterprises constituted a threat to the social and economic security of Canada. To ensure that the Service's activities were consistent with its mandate, however, its investigations were restricted, as a matter of policy, to the collection of "strategic" intelligence. The Service was to avoid involvement in individual criminal investigations.

In Part I of our review, the Committee noted that these limitations were not fully understood by some members of the RCMP who had expectations about the level of Service involvement that the Service was not prepared to meet. Our Part II inquiries at the regional and operational levels show that the misconception about the Service's role in transnational crime is ongoing.

It was evident to the Committee that the volume of relevant intelligence provided to the RCMP was relatively small. We were advised that there had been scrupulous adherence to the policy of restricting investigations to the strategic level. However, on the part of the RCMP officials concerned, the notion of "strategic" versus "tactical" investigations was still not clearly understood, and skepticism was expressed about the distinction having any validity. Several RCMP officials maintained that CSIS was withholding intelligence on transnational criminal activity from them—an accusation Service officers strenuously denied. We saw no evidence that intelligence was deliberately withheld from the RCMP. We address the

Our inquiries at the regional and operational levels show that the misconception about the Service's role in transnational crime is ongoing.

The CSIS-RCMP relationship can be characterized as one of genuine and fruitful cooperation.

matter further in our report on Transnational Criminal Activity on page 5.

Perhaps more serious was the fact that some RCMP officials regarded the CSIS material with the same suspicion as other shared CSIS information and were reluctant to request disclosure for the same reasons. It is the Committee's view that these problems have the potential to impair Canada's efforts to control this most invidious form of organized crime. We urge the Service, the RCMP, and the Government to take appropriate action to prevent future misunderstandings.

The Quality of the

Overall Working Relationship

The complaints SIRC researchers heard from the RCMP officials in all three divisions they visited were for the most part directed at Service policies or the wider administrative system which they saw as creating unnecessary difficulties. The Committee heard no specific complaints about officials of the Service. A number of RCMP officials were complimentary about the Service's overall contribution to joint operations and investigations, and to the level of cooperation generally. Meetings and familiarization sessions involving both agencies were frequent (mainly initiated by CSIS officials) and there was an ongoing informal process by which issues local to the region or division were usually resolved through personal contact between senior managers from both agencies.

There continues to be some residual friction in two regions over especially difficult cases that arose in the recent past. However, the Committee believes that there has been

no ongoing impairment to operational effectiveness. It is the Committee's view that with the exception of the two concerns set out above—RCMP use of CSIS intelligence in criminal proceedings, and CSIS responsibility in the area of transnational crime—the CSIS-RCMP relationship can be characterized as one of genuine and fruitful cooperation.

CSIS Liaison with Foreign Agencies

Report #112

Methodology of the Audit

Under section 38(a)(iii) of the *CSIS Act*, the Security Intelligence Review Committee reviews the foreign arrangements entered into by CSIS with foreign intelligence and police agencies, and monitors the flow of information to agencies with which CSIS has arrangements.

This year, we audited two posts that have witnessed significant political and economic changes in their areas of responsibility, and which are instrumental in the collection of information on regional conflicts and terrorism. The posts examined cover a heterogeneous range of countries, most of which are developing nations. Although a few adhere to democratic principles of government, political instability is a characteristic common to most of the countries concerned, and many can be found on the watch lists of human rights observers.

The review encompassed three main categories of material:

- All exchanges of information handled by CSIS Security Liaison Officers (SLOs) at the two posts, including electronic exchanges;
- All correspondence with foreign intelligence agencies handled by the posts; and
- All instructions and reference materials provided to and originating with the SLOs, including their “Assessments of Foreign Agencies.”

The essential goals of the review were to ensure that relationships and contacts with the foreign agencies concerned corresponded to the specific liaison agreements in place, and that information disclosed to foreign agencies or received from them was properly handled by the Service. Throughout, the Committee paid particular attention to information exchanges with agencies of countries suspected of human rights abuses.

Foreign Liaison Program

For the period under review, there were no major changes to the organization of the Foreign Liaison and Visits Branch (FLV) in the wake of its establishment as a “stand-alone” branch in mid-1997. However, several management issues came to our attention.

The “Third-Party” Rule for Information Requests

It is matter of general CSIS policy on the transfer of intelligence information that foreign agencies should not be acting on behalf of other agencies (domestic or international) when making information requests. It is essential to the transparency and integrity of the dissemination process that CSIS

know where information is going and who is asking for it.

Our review did identify several instances where the intelligence service of an allied country offered to act as a “broker” with agencies in other countries for information that CSIS was seeking. The Service did not accept these offers. Of a more serious nature, we learned of an instance where CSIS information was made available by the allied foreign agency to another intelligence service without permission from CSIS—an unambiguous violation of the “third-party” rule. The records show that CSIS Headquarters took a dim view of the practice and advised its SLOs to make clear to the foreign agency that it should cease these activities.

Yearly Reviews of Overseas Posts

In October 1996, the then manager of the Service’s foreign liaison program stated that he intended to conduct a yearly review of selected foreign liaison posts to aid the formulation of recommendations for improvements to Service executives. The Committee concurred in this decision.

Since then, however, we have determined that no formal plan has been implemented. While the current Director General of the Branch continues to inspect posts on a case-by-case basis as needed, we are of the view that the original proposal for a formal and regular reporting process has advantages over the current approach. The Service holds the view that the current monitoring process is adequate.

It is matter of general CSIS policy on the transfer of intelligence information that foreign agencies should not be acting on behalf of other agencies.

The establishment of liaison arrangements with foreign intelligence services must be approved by the Solicitor General.

A Revised Role for Security Liaison Officers

In previous audit reports, the Committee had supported a plan to give an active role to SLOs in the process by which information to be disseminated to foreign agencies was reviewed. Under this plan, Security Liaison Officers were to act, in effect, as a last check on the appropriateness of transmitting items of intelligence to other services. We were pleased to learn that the FLV Branch has made the plan operational.

Under the new policy, a Security Liaison Officer who disagrees with the proposed release of information to a foreign agency by the relevant CSIS operational branch can seek the assistance of the Headquarters FLV Branch in order to resolve the issue. The revised policy effectively revives a management function abandoned when the former Foreign Liaison Branch was disbanded in the early 1990s.

Foreign Liaison Arrangements

Foreign liaison is governed by individual arrangements under section 17 of the *CSIS Act* between the Service and foreign intelligence services, and by a 1982 Ministerial Direction. The Direction covers contacts and exchanges by Security Liaison Officers abroad as well as visits by CSIS or allied service personnel.

The 1982 Ministerial Direction on foreign liaison states that CSIS cooperation with a foreign agency must be compatible with Canada's foreign policy. Further, the establishment of liaison arrangements with foreign intelligence services must be approved

by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade.

A Comprehensive Review of All Arrangements

In recent years, the Committee has devoted considerable attention to the Service's foreign arrangements. *Inter alia*, the Committee has identified SLO reports that favourably rated disreputable and discredited agencies, and highlighted arrangements that had been left dormant for many years. In the most recent audit report (1997-98), we noted that fully one-half of the Service's 215 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS and, of these, many pre-dated even the 1982 Ministerial Direction.

With respect to an anticipated Government review of the arrangements as a whole we stated in 1998: "The imminent release of new Ministerial Direction will ... provide the opportunity to ensure that all foreign arrangements, particularly those that pre-date the Service, are reassessed and annotated." In furtherance of that end, the Committee also recommended that CSIS systematically reexamine all foreign arrangements following the release of the new Direction. However, as of August 1999 no new Ministerial Direction had been issued.

The Review Committee is concerned at this delay. The existing Ministerial Direction governing foreign arrangements is sadly out of date and a long-overdue comprehensive review of the arrangements is contingent on

the issuance of revised Direction. We strongly urge the Ministry to replace the 1982 Ministerial Direction with one that reflects the Government's experience with the administration of foreign liaison arrangements to date, and that is consistent with the *CSIS Act*.

New Foreign Initiatives

In the period under review, CSIS has been involved in a number of new initiatives which broaden the range of activities arising from its foreign arrangements. The Service established an intelligence training program for foreign agency personnel. The course provides instruction in intelligence analysis and insight into intelligence agency functions within democratic civil institutions. In addition, the Service rendered assistance to several foreign agencies seeking information about the drafting of legislation that would govern intelligence operations in their home countries.

Human Rights in Several Foreign Agency Relationships

Given the past records of some of the foreign agencies under the purview of the posts we examined, the issue of human rights took on even greater importance in our reviews. At one post, the only agency where an agreement was in place to exchange security intelligence information (as distinct from other, less sensitive materials) has had a poor human rights record. SIRC staff paid special attention to the information exchanges between that agency and CSIS, however, none of the information exchanged gave rise to concerns.

A foreign arrangement with a second agency, though more limited in the nature

of the information that could be passed, also drew the Committee's attention. Our concern was not with the agency directly, but rather with the potential for information to find its way to counterparts in the military and the police sectors.

The Service holds a relatively sanguine view of such exchanges, maintaining that most intelligence agencies are without enforcement powers and so are less often human rights offenders. While the Committee acknowledges this point, we believe continued caution is in order. CSIS may give information to an agency that does not violate human rights, however, that agency could in turn pass the data on to other organizations of government that do. In the case at hand, we saw no problematic information exchanges from CSIS to the foreign agency.

With respect to a third agency with a poor human rights record, we took special care to examine the exchanges of correspondence. The Committee noted that the Service was fully cognizant of the allegations of corruption, incompetence, and human rights abuses, and that it had taken this knowledge into account in the management of the relationship. The Service informed us that the relationship was contingent on the continued satisfactory human rights conduct of the foreign agency.

A Foreign Arrangement of Special Sensitivity

An arrangement of several years standing between the Service and a foreign intelligence service in a country with a history of major human rights abuses drew the Committee's particular attention.

The existing Ministerial Direction governing foreign arrangements is sadly out of date.

The Service informed us that the relationship was contingent on the continued satisfactory human rights conduct of the foreign agency.

Approved by the Solicitor General, the arrangement was quite limited in scope. Incorporated into the terms of the arrangement was the provision that after a relatively short period, the agreement would be reviewed. In addition, in order to protect nationals from the government of the state concerned, CSIS was instructed not to seek information from the foreign authorities about persons still living inside that country.

In accordance with the instructions from the Minister, CSIS reviewed the relationship and, having found it useful and beneficial to Canada, the Service asked the Minister to renew it. The Solicitor General did so, with the proviso that CSIS again review the arrangement and report one year hence. When the Committee set out to verify whether CSIS had in fact complied with the Minister's instruction for another review, we determined that it had not. We were informed by the Service that they believed the instruction had been given in error.

Following consultation with the Ministry of the Solicitor General, the Committee determined that notwithstanding the Service's interpretation, the Minister's instruction was both clear and valid. The Service was obliged to review the arrangement and return to the Minister for approval. The Service has since informed us that it has written to the Solicitor General seeking approval for the arrangement.

A General Comment on Human Rights and Foreign Agencies

The essential purpose for having arrangements with foreign intelligence agencies is to allow CSIS to collect information that will protect

Canadians. In the ideal world, the Service's foreign contacts would all have satisfactory human rights records—the reality is that many do not. In order to obtain the information it needs CSIS sometimes has to deal with agencies having poor human rights records.

The Committee believes that all possible care should be taken to make sure that the Service's exchanges of information are not used to assist in the violation of human rights. In order to ensure that the dissemination of information is tightly controlled, SLOs must make available to the rest of CSIS timely and accurate information about an agency's human rights record, as well as its propensity to pass information onto third parties without authorization.

Cooperation Outside the Terms of an Arrangement

Upon reviewing files detailing the information exchanged with two foreign intelligence services, we identified types of information disclosed by the Service that fell outside the limits set by the arrangements.

The disclosures took place when CSIS was informed about a plan to engage in terrorist campaigns against foreign officials. In view of the urgent nature of the information, the SLO received permission from CSIS Headquarters to disclose the information to officials of the foreign government concerned.

The Director of CSIS informed the Solicitor General of the matter. While it is clear that the disclosure of the information went beyond the scope of the liaison arrangements, Ministerial Direction gives the Director the prerogative to authorize disclosures in exceptional

circumstances. The Committee believes the Service acted properly in this case.

Dated Information

As is common practice among intelligence services, CSIS requires that its Security Liaison Officers overseas file reports on their activities and generate assessments of the agencies with which they interact. Our review of the files of one of the posts we audited revealed that key administrative reports were considerably out of date.

The importance of these reports should not be underestimated since they are a key tool enabling Headquarters staff and CSIS executives to make decisions on what should be disseminated to foreign agencies. The Committee regards this deficiency as more than a mere administrative detail. The Service has informed us that remedial actions were taken to update the files, and measures put in place to help prevent stale-dated assessments from being circulated in the future.

Dissemination to Another Agency of Government

In this instance, the Committee examined the Service's investigation of several foreign nationals who were suspected of having participated in an overseas program that threatened Canada's national security. The Service had concluded that the suspects posed no threat, yet appeared to have passed information it collected about the persons to another agency of the Canadian government. The Committee inquired of the Service about the nature of the information disseminated and the authority under which the transmission was carried out. The Service advised the

Committee of the circumstances and the Committee was satisfied that the exchanges of information had been properly conducted.

A Case Under Review

A Committee review of the instructions from CSIS Headquarters to one of its SLOs seemed to indicate that an overseas officer was being asked to conduct an investigation of the kind which would have required prior Ministerial approval. No such approval had been sought and we conducted further inquiries into the issue.

Our conclusion was that CSIS Headquarters had not intended its instruction to be read as—nor did the SLO interpret it as being—a “tasking” to conduct an investigation. Instead, the apparent purpose of the Headquarters query was to make the SLO mindful of a particular situation during his discussions with other foreign representatives abroad so that any relevant information gleaned could be incorporated in ongoing updates of agency assessments.

Having informed the Service of our concern about the ambiguous communication, we noted an early response to our queries. Service Headquarters staff have since been cautioned a number of times about the need for increased diligence and precision in communications with SLOs.

A General Finding

The Committee's periodic reviews of the Service's overseas liaison activities encompass all the many difficulties associated with work in foreign posts. SLOs sometimes face environments which are personally and professionally challenging. In general, the SLOs in the two

Our review of the files of one of the posts we audited revealed that key administrative reports were considerably out of date.

posts reviewed demonstrated initiative, employed good judgement, and the Service exercised appropriate restraint in deciding what information would be shared with its foreign partners.

Areas of Special Interest - Brief Reports

Allegations by a Former CSIS Employee (S. 54)

Report #113

Under section 54 of the *CSIS Act*, the Solicitor General may at any time ask the Committee to report on a matter relating to its mandate. In July 1998, the then Solicitor General, the Honorable Andy Scott, advised the Committee of certain allegations against CSIS by a former employee of the Service. The Minister asked us to report on the matter, reviewing the allegations and detailing the facts, if any, on which the allegations were based.

The allegations were diverse in character: abuse of power, systemic abuse, nepotism, corruption, favoritism, sexual harassment, and non-compliance with the Service's policies and Canadian law. Four additional allegations concerned CSIS operations.

The Committee's research officer met with the complainant, however, he refused to provide details of his allegations on the grounds that he did not believe in the integrity of the process. Thus for details of the complainant's allegations we relied

upon letters written by the complainant prior to the commencement of our inquiry.

The former employee's concerns appeared to originate in the Service's dismissal of a grievance filed in 1987. The Committee took special note of a letter sent subsequently to the Director of CSIS in which the complainant stated that if the grievance were to be settled in his favour, the additional allegations—even the most serious ones—could be somehow resolved. However, if a settlement of the grievance in his favour was not forthcoming, he would resort to using other information in his possession that would in his words “take care of the Director's hesitations.”

Notwithstanding the Committee's view of this statement—effectively an attempt at blackmail—we took all of the complainant's allegations seriously and investigated each one.

In its report, the Committee took care to note to the Minister that with respect to the human resource elements of the inquiry, we were fully aware that the Service's personnel management policies lay outside the Committee's normal powers of review and investigation. Nevertheless, we were able to reach some very clear findings.

Overall, we concluded that the allegations were unfounded. The salient findings of our report to the Minister are presented below:

- Contrary to the former employee's claims that many CSIS positions were staffed on a non-competitive basis, our study determined that in fact very few were

filled by appointment, and none of those who occupied such positions had previously been employed as executive assistants as alleged by the complainant.

- We reviewed the staffing strategy as outlined in the Service's human resources policy manual. After examining all available background documents, candidate qualifications, and hiring procedures we concluded that an allegation concerning a 1997 competition in Montréal was completely unfounded. All personnel practices in this case were consistent with the established policies.
- In respect of the complainant's allegations of sexual harassment involving classes of new CSIS recruits, the Committee concluded that they too were not supported by the facts.
- The complainant made an allegation about the Service's response to a harassment complaint against one of its managers. Our review turned up no inappropriate actions in the way CSIS dealt with the complaint.
- On the issue of the Service's mandatory mobility clause for intelligence officers, we believe (unlike the complainant) the policy to be essential both for operational and professional development purposes. It would be difficult to imagine the viability of a national intelligence agency in the absence of such a personnel management policy.
- We were particularly concerned by the complainant's allegation that operational information had been collected during the course of security screening interviews for Citizenship and Immigration Canada. As noted in earlier audit reports, such allegations touch one of the Committee's special concerns. Unfortunately, this allegation was very broad and came to us unsupported by examples or details. While the paucity of details left the Committee with little to investigate in this instance, we are reassured by the fact that we routinely examine the context and content of reports following screening interviews, and that we are able to investigate thoroughly when detailed complaints are made.
- The Committee's report to the Minister also took issue with the former employee's highly tendentious view of one of the Service's former directors. We were especially disturbed by the cavalier manner in which the reliability and loyalty of a work colleague with a very impressive track record in Government service in Canada and abroad was called into question by the former employee.
- And finally, with respect to one of the more serious allegations concerning operational matters, the Committee determined that a claim that a CSIS director had deliberately concealed information from review agencies (SIRC and the Inspector General) reviewing the Service's role in the 1992 Iranian embassy attack was entirely unfounded.
- All the other allegations of an operational nature were found to be without merit.

We were especially disturbed by the cavalier manner in which the reliability and loyalty of a work colleague...was called into question by the former employee.

Although we found CSIS' file review process to be sound, we did find problems in the Service's implementation of that process.

Overlooked Files

Report #116

In early 1998, while conducting file reviews at CSIS Headquarters, the Committee came across files that were opened by the RCMP Security Service, and which had been overlooked during the Service's major review in 1990 of all of the files inherited from the RCMP. These files were still considered "active", even though their retention periods had expired and they were to have been assessed for disposal.¹¹

Following our queries, CSIS conducted an internal review and found 833 files that had been missed by their review procedures. The Service concluded that a number of these files were still of operational value. We examined a sample of these files to assess the Service's rationale for retaining them.

Our review of the files revealed that the misplacing of the files was an "administrative oversight": they had inexplicably not been assigned a Bring Forward (BF) date during the Service's 1990 major review.

In general, although we found CSIS' file review process to be sound, we did find problems in the Service's implementation of that process.

Although we were informed that CSIS issued a procedures booklet in 1995, we observed that the Service's *File Review and Disposition Guidelines*, developed to assist analysts in their file disposal decisions, had not been updated since they were last amended in 1991.

We recommend that the *File Review and Disposition Guidelines* be updated to reflect the Service's present policy and operational requirements.

The Service informed us that it would review and update its disposition procedures.

Our review showed that when the National Archives Requirements Unit (NARU) referred disposal decisions on files to the relevant operational desks, no process existed for follow-up.

We recommend that the operational units be required to comply with NARU deadlines for disposal decisions, and that NARU establish an effective follow-up process.

CSIS said that it would establish a new BF system.

We found that the analysts' written rationales to retain files seldom referred to the specific retention criteria listed in the Guidelines. We also observed that the written rationales that were provided to support retention were not sufficiently detailed.

We recommend that analysts in NARU and the operational desks provide detailed rationales for their decisions to retain files, citing the applicable criteria listed in the Schedules and the Service's interest pursuant to the *CSIS Act*.

Finally, in our view, a number of files should have been transferred to the National Archives of Canada, or even destroyed, because they did not appear to contain information of operational value. We have so informed the Service.

A Foreign Conflict Case

Report #106

In 1998-99, SIRC reviewed a complex and sensitive human source operation conducted over several years by the Service. Because of the high level of secrecy associated with the operation, we are constrained by national security from providing details that might put lives in danger. The Committee did find, however, that it disagreed with CSIS on significant aspects of the conduct of the operation and we have communicated our views on these difficult issues to the Director of CSIS.

SIRC View of Issue-Based Targeting

In recent years the Review Committee and others (notably the Inspector General of CSIS) have become seized with the difficulties potentially created by a form of investigation called “issue-based” targeting. This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects that there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not yet been identified. In other words, the targeting authority allows CSIS to investigate the general threat, and to try to identify the

persons or groups who are taking part in threat-related activities. As in any other targeting procedure, if warrant powers are involved, approval must be granted by the Federal Court.

A hypothetical case necessitating issue-based targeting could occur if, for example, a series of bombs were being exploded across the country, with no particular group claiming responsibility. CSIS would investigate under an “issue-based” targeting authority, the legal foundation for which would be the suspicion that there was a threat to the security of Canada as defined in section 2 of the *CSIS Act*.

The investigation might reveal that the bombs were the result of domestic criminal activities alone. Alternatively, it could show that a politically motivated group had decided to use violence to help achieve its political objectives. In the first case, CSIS should hand over all of its information to the police and cease its own investigation. In the second, CSIS would continue its investigation and as information became available, the investigation would be narrowed to the individuals or groups directly concerned.

The alternative to issue-based targeting in the example cited above is that CSIS would attempt to find out what was going on, and who was making and detonating explosive devices, but would do so—and this is the crucial distinction—in the complete absence of any formal targeting process and its attendant legal and administrative procedures. The differences between the two approaches might not seem very important when something as

We urge the Service to make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable.

concrete as exploding bombs is the context, but it could be most important in other less clear-cut situations.

It is the view of the Committee that issue-based authorizations are far preferable to none at all. We would take active exception to a CSIS policy that allowed any investigative activity at all to take place without an appropriate targeting authority.

While the Committee does believe that there is a place for issue-based targeting in the array of options legally available to CSIS in carrying out its responsibility to protect the safety and security of Canada, we add the caveat that investigations under such authorities should be carefully monitored by senior management. Additionally, we urge the Service to make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable.

The Review Committee will continue to pay special attention to this kind of investigation so as to assure ourselves that all are being conducted appropriately.

comprehensive examination such as this provides insight into the various types of investigative tools the Service has at its disposal, and permits the Committee to assess how new Ministerial Direction and changes in CSIS policy are implemented by the operational sections of the Service.

The Targeting of Investigations

The targeting section of the regional audit focuses on the Service's principal duty—security intelligence investigations authorized under sections 2 and 12 of the *CSIS Act*. When examining any instance in which CSIS has embarked on an investigation, the Committee has three central concerns:

- did the Service have reasonable grounds to suspect a threat to the security of Canada?
- was the level of the investigation proportionate to the seriousness and imminence of the threat?
- did the Service collect only the information that was strictly necessary to advise the government on the threat?

Committee researchers also keep watch generally on the manner of the Service's adherence to its own internal operational policies, rules, and directives.

B. Annual Audit of CSIS Activities in a Region of Canada

Report #111

Every year the Committee audits the entire range of CSIS investigative activities—targeting, special operations, warrants, community interviews, and sensitive operations—in a particular region of Canada. A

Methodology of the Audit

In the region at issue, the Committee selected eight investigations—six counter terrorism cases and two counter intelligence cases. Of the eight, three were issue-based investigations. SIRC researchers reviewed all files and operational messages in the Service's electronic

Management of Targeting

Target Approval and Review Committee

CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada, and are related to or emanate from that specific issue.

data base. Researchers also interviewed the CSIS officers who carried out the investigations as well as their managers.

Findings of the Committee

In all eight cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The targeting levels were proportionate to the seriousness and imminence of the threats in all but one case, and no actions were taken against non-targets. The Committee concluded that in all of the cases we reviewed, the Service collected only the information that was strictly necessary to advise the government about the threats.

In three instances, however, the Committee had reservations about the accuracy of some of the information presented to the Target Approval and Review Committee (TARC). We suggested to the Service that it take measures to enhance overall quality control of the information provided to TARC.

The cases which raised issues and concerns for the Committee are summarized below.

Targeting Level

The first case involved a counter terrorism investigation pertaining to a landed immigrant's involvement with a known terrorist group and his activities within an ethnic community in Canada. The person had been

The Regional Office used its investigative powers with parsimony and in proportion to the threats posed.

under investigation for a number of years and during the period under review the Target Approval and Review Committee had authorized a higher level of investigation.

The Service's justification for requesting a higher level investigation was that it had information that the target's expertise was being sought by leaders of a known terrorist group, and that he had contacts with those leaders. However, our review showed that the Service had not collected information that in our opinion supported the more intrusive investigation. We believe that the original lower-level targeting authority was sufficient to address the threat posed.

Termination of an Investigation

The second case involved a counter terrorism investigation of an individual in relation to the activities of a known terrorist group based abroad and with representatives in Canada. We agreed that the Service had reason to suspect the individual of activities that posed a threat to Canada. The target's behaviour lent credence to the Service's interpretation of the facts as presented to the Target Approval and Review Committee.

Our review showed that the Service's investigation revealed no pattern of terrorist activity, and that CSIS had quite properly terminated its investigation upon reaching that conclusion.

Accuracy of Facts Presented To The Target Approval and Review Committee

Case three concerned a counter terrorism investigation of an individual whose activities came to the attention of the Service as part of a wider investigation into a known terrorist

group present in Canada. While we concurred with the Service's view that the target's relationship with known terrorist figures constituted a potential threat to Canada, we took issue with one part of its Request for Targeting Authority (RTA).

In a manner which bolstered the Service's case for the authority, the targeting request presented a fact that was not consistent with the information collected. When questioned by the Committee, the Service acknowledged the error. The Committee was of the view, however, that the discrepancy did not undermine the legitimacy of the targeting authorization.

Three Issue-Based Investigations

Cases four, five and six, were all issue-based investigations, two from counter terrorism and one from counter intelligence. In both counter terrorism investigations, the Committee found that CSIS had met the test of "reasonable grounds to suspect" in justifying its inquiries, that CSIS had collected only information that was strictly necessary and that there was no extensive reporting on individuals who were not already the subject of specific targeting authorizations. In sum, for these two cases, the Committee believes that the regional office used its investigative powers with parsimony and in proportion to the threats posed.

An Investigation of Economic Espionage

The Committee reviewed a case involving economic espionage. Investigations of economic espionage are conducted under section 2(a) of the *CSIS Act*, and Ministerial Direction notes that for the activities to warrant investigation they must be against

Canada (assets, policies or programs of the Government of Canada) or detrimental to the interests of Canada.

Since the Service's request for this investigation did not explicitly list Government assets or programs, its request fell under the "activities...detrimental to the interests of Canada" criterion. Ministerial Direction further specifies that in instances where it is unclear if the activities have a negative impact on the "national interests," the Service should seek guidance from another government department or agency.

Our examination of the information submitted to TARC in order to obtain a targeting authorization turned up an error of fact and two points we believe were overstatements in relation to intelligence reports on which the submission was based.

Obtaining and Implementing Federal Court Warrants

Under section 21 of the *CSIS Act*, only the Federal Court of Canada can grant CSIS the right to use warrant powers, such as telephone or mail intercepts. In requesting such powers, the Service must present an affidavit to the Court attesting to the facts which require their use. Every year, the Committee audits a number of affidavits by comparing them with information in the Service's files. In reviewing warrant affidavits, the Committee is focused on three central questions:

- do the facts presented in the affidavit accurately reflect the information used as the basis for its preparation;

- is the case that the Service presents to the Court set out in its proper context; and,
- are the facts, circumstances and statements of belief contained in the affidavit fully, fairly and objectively expressed?

1997-98 Developments Affecting the Warrant Process

As part of its audit, the Committee also reviews changes in Ministerial Direction and CSIS policy for the relevant period which govern the application for and implementation of warrant powers. We also examine all Court decisions that might impact upon the Service's use of warrant powers, as well as any significant changes to conditions accompanying the warrants.¹²

In 1997-98, there were no new Ministerial Directions or instructions pertaining to warrants. However, there were changes to CSIS policies and new Court decisions of interest.

Changes to CSIS Policies

As a result of restructuring at the Executive Level of CSIS, changes were made to the roles and responsibilities of certain officials in regard to warrant applications and the execution of warrant powers. The responsibilities include verifying that the warrant applications comply with Service legal and policy requirements, ensuring that the necessary resources are available to execute the warrants, checking that each application is processed on a timely basis, and approving all operations involving the powers granted by the Federal Court.

We also found that the Service amended its policies to tighten the controls in regard to intercepts of solicitor-client communications.

Only the Federal Court of Canada can grant CSIS the right to use warrant powers.

The Service has been employing greater precision and rigour in the preparation of its warrant applications.

New Court Decisions

Two Warrant Denials

In last year's report, the Committee commented on the Federal Court's denial of a small number of warrant applications. We reviewed these Federal Court decisions and found that the warrant applications were rejected because they did not meet the threat requirements of paragraphs 2(a) or 2(b) of the *CSIS Act*. We also learned that the Service later went back to the Federal Court with revised applications and the warrants were granted.

While the Committee did not identify any specific impacts of these decisions on the operational activities per se, we did observe that in accommodating the evolving judicial review process, the Service has been employing greater precision and rigour in the preparation of its warrant applications.

Changes to a Warrant Clause

In 1997-98, in what appeared to be another iteration of the McGillis decision,¹³ the Federal Court removed the "reasonable

grounds to believe" statement found in a certain clause. The amendment removed the discretion previously granted to senior Service officials in authorizing the execution of warrant powers against a certain type of target. The effect was to compel the Service to meet a higher threshold of certainty in the facts that it put before the Court. The Service subsequently deleted the particular statement from similar clauses found in all its warrant applications.

Content of Affidavits

In 1997-98, the Federal Court requested that certain sources of information provided in support of warrant applications be specifically identified in the affidavits. We were informed that this practice was adopted by the Service for all subsequent affidavits.

Findings of the Committee

Warrant Preparation

From a comprehensive listing of all warrants executed in the region for the period under review, the Committee chose three applications relating to two target groups in the

The Warrant Process

In order to obtain warrant powers under Section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court with a sworn affidavit justifying the reasons why such powers are required to investigate a particular threat to the security of Canada. The preparation of the affidavit is a rigorous process involving extensive consultations with the Department of Justice, and the Solicitor General, with the latter's approval being required before a warrant affidavit is submitted to the Court. The facts used to support the affidavit are verified during the preparation stage and reviewed again by an "independent counsel" from the Department of Justice to ensure that the affidavits are legally and factually correct prior to the submission to the Federal Court. This process has evolved over the past several years with a view to ensuring that the facts, and statements of belief based on those facts, are accurate.

counter terrorism area.¹⁴ Among these, we identified a number of statements made by the Service which accurately reflected neither the operational nor the open source information available to the Service.

In the first application we reviewed, our initial findings were that there were a large number of inaccuracies and unsubstantiated statements in the affidavit. The Service subsequently provided the Committee with additional material to substantiate the problematic allegations. We reviewed the additional material and found that most of the allegations were, in fact, substantiated by the documents provided by CSIS.

However, certain allegations remained of concern and, in our view, were not an accurate reflection of the operational and open source information available to the Service: the affidavit presented a confused picture regarding the source of certain information, and some information lacked corroboration.

The other two applications also contained several allegations that were not, in our view, sufficiently supported: the known facts did not lead to the Service's conclusions, support for certain facts was insufficient or the allegations were based on outdated information. With respect to the two latter problems, the Service reached a similar view. We were informed that in the last case, the statement we questioned was not included in the subsequent warrant application against the target group.

With respect to the warrant preparation process in general, the Committee remains

seized with the issue. In two previous reports we have noted deficiencies in some past CSIS applications for warrant powers. Since proper affidavit preparation is key to the integrity of the targeting and investigatory process, it is a matter the Committee regards with utmost seriousness.

We noted that among the warrant applications reviewed for this and previous audits, the recent affidavits were much improved in all respects. The Committee is hopeful that these improvements reflect the refinements made of late to the Service's warrant preparation process.

Warrant Implementation

The Committee reviewed the Service's use of warrant powers in the region and found that their implementation complied with all of the terms and conditions contained in the warrants.

Warrant Tracking

The process by which CSIS tracks warrant applications is also of interest to the Committee. Kept in diary form, the records of the warrant process provide additional assurance that all mandated procedures have been correctly followed. For the period under review, the Committee identified no anomalies in the warrant tracking records.

Quality Control in Reporting

Because intercept reports can provide the basis for requests to continue warrant operations and for targeting authorities, the accurate reporting and transcription of material generated by warrant intercepts is vital.

Since proper affidavit preparation is key to the integrity of the targeting and investigatory process, it is a matter the Committee regards with utmost seriousness.

We reviewed all requests from the Service for Ministerial approvals involving operations in the Region, and all requests to senior managers involving “sensitive institutions”.

In this year’s regional audit we found that the region in question was conducting quality control audits in accordance with the 1997 national draft policy.

We learned that the region had taken steps to ensure the quality of the reporting done by its analysts. For example, the quality control program in the region not only offered training to new analysts on quality reporting, but conducted regular performance evaluations and formalized assessments through audits.

Audit of Sensitive Operations

The very nature of sensitive operations dictates that they are subject to relatively frequent Ministerial Direction. In addition, policy for implementing sensitive operations is set out in some detail in the *CSIS Operational Policy Manual* and all requests for sensitive operations, depending on the level of sensitivity, require the approval at the very least of Service senior management.

In the course of the Committee’s regional audit, we examined a set of randomly selected human source operations. In addition, we reviewed all requests from the Service for Ministerial approvals involving operations in the Region, and all requests to senior managers involving “sensitive institutions”—that is, operations touching on legitimate dissent, illegal activities, and certain other matters.

Findings of the Committee

Although the policy implications of one case initially concerned us, we ultimately concluded that all source operations we intensively examined complied with legislation and Ministerial Direction. We will, however, pursue further inquiries about another investigation that had come to our attention during this review.

Internal Security

Breaches of internal security can have a catastrophic impact on an intelligence service and upon the security interests the agency is meant to guard. In CSIS, internal security is the responsibility of the Director General of Internal Security, who directs internal security officers at Headquarters and in each regional office. When it is determined that a security breach has taken place, the Director General or her representatives, investigate and recommend remedial measures.

For the fiscal period 1997-98, the Committee examined cases of suspected and actual security breaches in one region, and reviewed the security measures in place in the same regional office.

Breaches of Internal Security

We found several security issues that concerned us. In the first instance, a Service employee had inappropriately disclosed operational information. We had qualms about how CSIS had conducted its investigation. In pursuing our review, we received an

extensive explanation by CSIS about its actions, and we asked the Director to personally respond to questions about the management of the case. We learned that the matter had been considered at the highest levels of the Service.

mate need for most of the access requests, although some minor security violations were identified. The other allegations of security violations proved to be unfounded.

After duly considering all of the information, we concluded that CSIS had taken appropriate action and had handled the case in a fair manner.

The second case involved the temporary loss of classified information. The incident arose from the mistaken belief among employees that they needed to follow certain procedures when transferring information. Following the incident, CSIS changed its procedures for handling data, and provided corrected instructions to its employees.

We also examined other less serious cases. Among them were allegations of unauthorized browsing in the CSIS computer data base. In one case, the internal investigation determined that the employee had a legiti-

Table 1
New and Renewed Warrants

	1996-97	1997-98	1998-99
New Warrants Granted	125	72	84
Warrants Renewed/Replaced ¹⁵	163	153	163
Total	288	225	247

granted and the nature of the targets listed provide insight into the entire breadth of CSIS investigative activities and are an important indicator of the Service's view of its priorities.

We compile statistics based on a quarterly review of all warrant affidavits and warrants granted by the Federal Court. Several kinds of information are tracked annually, such as the number of persons and number of locations subject to warrant powers. This format continues a practice established prior to the *CSIS Act*. Table 1 compares the number of warrants over three fiscal years.

Findings of the Committee

While the data provides the Committee with an excellent profile of the Service's requests for warrant powers in a given year, comparisons year-to-year are less enlightening, because the applications vary as a result of legal decisions by the Courts and new developments in technology. In addition, raw warrant numbers can be misleading since one warrant can authorize the use of a power against one or many persons.

Despite these variables, however, the Committee concluded that measured overall, the total number of persons affected by CSIS warrant powers remained relatively stable for the last two years, and foreign nationals continued to represent the overwhelming majority of persons subject to warrant powers.

Regulations

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies for warrants. In 1998-99, no such regulations were issued.

Federal Court Warrant Conditions and Other Developments

Warrant Conditions

Most warrants authorized by the Federal Court contain conditions which limit the use of warrant powers and which the Service must follow in their execution. In 1998-99, the Federal Court instructed CSIS to:

- add a new condition pertaining to the destruction of video images of persons who are not targets; and
- revise an existing condition to limit the Service's discretion to intercept targets at certain locations.

We learned that in 1998 CSIS commenced a complete review of its warrants that will affect the clauses and conditions in all warrants. Some revised clauses and conditions have already been approved by the Federal Court. CSIS expects to complete the process in fiscal 1999-2000.

Court Denials of Warrants

In 1998-99, the Federal Court of Canada denied a CSIS application to replace expiring warrants. The Court rejected the application because it was not convinced that the requirements of paragraphs 21(2)(a) and (b) of the *CSIS Act* had been met.¹⁶ We understood that the Service was not planning to return to the Federal Court with a revised application.

New Court Decisions

In 1998-99, the Federal Court rendered two decisions which affected CSIS' use of certain warrant clauses.

In one case, the Federal Court instructed CSIS to delete a clause in a warrant that dealt with a particular type of target. Since the decision was specific to this case, it did not affect other warrant applications containing the same clause.

In the second case, the Federal Court found that a new wording of the Service's "resort to"¹⁷ clause with respect to a specific search power was overly broad and as such constituted an improper use of the clause. The Court also held it to be an illegal delegation of the authority of the Court. The clause allowed the Service to search a place not named in the warrant when it had reasonable grounds to believe an object or thing belonging to the subject of the warrant could be found at that location. CSIS has since removed this clause from new warrants and has advised its regional offices that they are not to make use of the clause where it occurs in existing warrants.

CSIS Operational Branches

Counter Terrorism Branch

The Counter Terrorism (CT) Branch is one of the two main operational branches at CSIS (the other being Counter Intelligence) and its role is to provide the Government of Canada with advice about emerging threats of serious violence that could affect the national security of Canada. The threat from international terrorism continues to be associated with what are termed "homeland" conflicts. Various domestic extremist groups are also regarded as potential threats to the security of Canada because of their capacity to foment violence.

During the year under review, we noted some significant changes (increases and decreases) in the number of investigations of potential threats from extremist groups in Asia and the Middle East. The Branch listed its priorities to be in the areas of chemical, biological, radiological and nuclear terrorism; cyber terrorism and threats to information operations; and fund raising for alleged terrorist operations. In addition, CT Branch continued to respond to significant domestic threats of violence.

The Committee finds it noteworthy that since the end of the Cold War, CSIS resources devoted to investigatory activities have been directed away from counter intelligence in favour of counter terrorism issues, such that CT currently consumes upwards of 60 per cent of the Service's budget.

Threat Assessments

CSIS provides threat assessments to departments and agencies within the Federal Government based on relevant and timely intelligence. CSIS prepares assessments—upon request or on an unsolicited basis—dealing with special events, threats to diplomatic establishments in Canada, and other situations. Threat assessments can play a crucial role, not only in advising authorities when an activity such as a demonstration is likely to degenerate into violence, but also in reassuring authorities when there is, in fact, little likelihood of violence.

In 1998-99, the CT Branch Threat Assessment Unit produced 683 assessments, up almost 20 percent from the previous year. The Service cited no specific reason for the increase. The volume of threat assessments

Since the end of the Cold War, CSIS resources devoted to investigatory activities have been directed away from counter intelligence in favour of counter terrorism.

depends on a variety of factors—the number of foreign visitors to Canada, requests received from other Government departments and agencies, special events, and threats received or developed over the year—all of which are beyond Service control.

Counter Intelligence Branch

The Counter Intelligence (CI) Branch monitors threats to national security stemming from the espionage activities of other national governments' offensive intelligence activities in Canada.

We reported last year that the Service had signed foreign arrangements with the intelligence agencies of some current and former adversaries in order to encourage them to act with more transparency and to explore common ground for cooperation and information sharing. In response to a Committee inquiry about the results of this ongoing effort, the Service reported that while it had set out no specific objectives, it regarded the process of establishing sustained and trusted relationships with foreign intelligence services as “never-ending.”

CSIS described the progress of these new

relationships as positive, slow, and cautious, involving the development of parameters for information exchange, focus on increasing the level of mutual trust, and regular reevaluation.

The Service told the Committee that Government fiscal restraints have had particular impact on activities. In the Service's view, current resources provide “little room for manoeuvre” in choosing which threats should receive special attention.

Analysis and Production Branch

In last year's report, the Committee stated its intention to conduct an in-depth study of the Service's Analysis and Production (RAP) Branch. The results of our review are found in Section 1, page 11.

The RAP Branch provides advice to government on the threats to the security of Canada through the production of CSIS Reports, CSIS Studies, and CSIS Intelligence Briefs. Table 2 shows the number of reports published by RAP in fiscal year 1998-99.

RAP produced a total of 68 reports, a slight decline from 73 issued in 1997-98. The Service's contribution to the Intelligence

Table 2
RAP Reports

CSIS Reports, Studies and Intelligence Briefs	Commentary	Intelligence Assessment Committee (IAC)
68	3	5 (Lead) 17 (Contribution)

Assessment Committee (IAC) remained essentially unchanged from last year.¹⁸ There were three issues of the Service's unclassified periodical *Commentary*.

Government Liaison Unit

The RAP Government Liaison Unit is the mechanism by which CSIS identifies the interests of government departments and agencies. An initiative of the Branch in 1997-98 was the publication of quarterly reports, for CSIS use only, detailing comments and feedback from the Branch's clients. The Committee noted with regret that this initiative was not pursued in 1998-99.

Arrangements with Other Departments and Governments

CSIS and the Royal Canadian Mounted Police

Among the most important of the Service's domestic arrangements is that with the RCMP. As an information addendum to the major two-part review of the relationship (See page 20) we present here developments in CSIS-RCMP cooperation for fiscal year 1998-99.

Information Exchanges

CSIS and the RCMP exchange information about their activities pursuant to their respective mandates: CSIS collects and disseminates information about threats to the security of Canada, and the RCMP carries out its mandated law enforcement functions in relation to the same threats.

Of the totality of written information

exchanged in both directions in fiscal year 98-99, CSIS was responsible for generating more than two-thirds. And three operational branches at Service Headquarters (Counter Terrorism, Counter Intelligence, and Analysis and Production) produced most of that volume.

CSIS-RCMP Liaison Program

The mechanisms to facilitate liaison and cooperation between CSIS and the RCMP are set out in the Memorandum of Understanding (MOU) between the two agencies. They include the assignment of liaison officers to national headquarters and to each of the regional offices.

Our review showed that during the relevant period, both agencies appeared committed to improving the liaison program. The Senior Liaison Committee—established as a forum to resolve problems and disagreements between the two agencies and defunct since 1993—was reactivated.

Revision of the CSIS-RCMP Memorandum of Understanding

In last year's report the Committee commented on the concerns expressed by both CSIS and the RCMP that the existing MOU did not adequately address the disclosure problems associated with the *Stinchcombe* decision. As part of an internal audit begun in the fall of 1998, the RCMP has undertaken a review of the CSIS-RCMP MOU. The Committee will monitor the results of this review for its potential impact on Service activities. We have observed that even in the wake of the *Stinchcombe* decision, the Service continues to provide a great deal of information to the RCMP.

Even in the wake of the *Stinchcombe* decision, the Service continues to provide a great deal of information to the RCMP.

Domestic Arrangements

In carrying out its mandate, CSIS cooperates with police forces, and federal and provincial departments and agencies across Canada. Pursuant to section 17(1)(a) of the *CSIS Act*, the Service may conclude written cooperation agreements with domestic agencies after having received the approval of the Minister. The Service is not required to enter into a formal arrangement in order to pass information to or cooperate on an operational level with domestic agencies. However, it is the usual practice for the Service to enter into a formal arrangement when the other party requires terms of reference or the setting out of agreed undertakings.

Currently, CSIS has nineteen formal MOUs with Federal Government departments and agencies, and eight with the provinces. CSIS also has a separate MOU with several police forces in one province.

Arrangements for 1998-99

The Service signed no new MOUs with domestic agencies in fiscal year 1998-99. However, the Service did receive Ministerial approval to conduct a number of security assessments for a provincial agency in advance of final authorization to conclude a future arrangement with that agency.

During fiscal 1998-99, the Service also made minor “housekeeping” amendments to an MOU it has with a federal department reflecting changes in contacts within and between the respective agencies. In accordance with an MOU’s termination clause, an arrangement with another federal agency

lapsed automatically in 1998. We were informed that after extensive consultations, the Service determined that renewal was not necessary.

In 1998, the Treasury Board made a budgetary transfer to the Service in order for it to take on the responsibility of providing security assessments for the Department of National Defence.

International Arrangements

Pursuant to subsection 17 (1)(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General—after he has consulted with the Minister of Foreign Affairs—in order to enter into an arrangement with the government of a foreign state or an international organization. During the initial phases leading to the approval of an arrangement, CSIS is not permitted to pass classified information to the foreign agency. However, it may accept unsolicited information.

Arrangements for 1998-99

During fiscal year 1998-99, CSIS received the Minister’s approval for three new liaison arrangements. Eleven existing arrangements were expanded during the same period. At the end of the fiscal year, CSIS had 215 liaison arrangements with 128 countries. There were also five liaison arrangements with three international organizations.

Of the 215 arrangements currently in force, the Service considers 39 to be “dormant”—a dormant arrangement being one in which there has been no contact for one year or more. Liaison agreements become dormant for a number of reasons: a simple lack of

need to exchange information, concerns by the Service about the other agency's professional or human rights practices, or an assessment that the political situation in the other country is too unstable.

Ministerial Direction

In a major study presented in last year's audit report ("CSIS Liaison with Foreign Agencies" p. 20) the Committee expressed the hope that what we believed at the time was the imminent release of new Ministerial Direction on foreign arrangement would address some fundamental problems in the area. However, the Committee is once again constrained to merely anticipate the new policies and hope that they deal with some of the issues we had raised.

As of July 1999, no new Direction had been forthcoming from the Office of the Solicitor General. The Committee continues to regard the revised instructions as vital, particularly in the face of the rapid increase in the numbers of foreign agreements between CSIS and foreign agencies during the past several years, and the fact that critical elements of the existing direction are out-of-date.

During our review this year of several liaison arrangements, we noted that the Foreign Liaison and Visits Branch sometimes did not have timely access to operational information which could have had an impact on decisions to enter into certain liaison arrangements. Although we were ultimately satisfied with the outcome of the arrangements reviewed, the Committee will continue to monitor future new arrangements to assure ourselves that the Foreign Liaison Branch has received complete and timely information.

A Problematic Foreign Arrangement

The Committee sought clarification from the Service about a new relationship approved by the Minister in 1997-98. The foreign intelligence services of the country concerned were involved in combating domestic terrorist forces, and the government itself had a very poor human rights record. However, CSIS also confirmed to the Committee that it had satisfied itself as to the foreign agencies' overall reliability.

An issue that did generate a statement of concern by the Committee pertained to the proper identification of all parties to a foreign arrangement. Ministerial Direction requires that all the agencies involved in an arrangement be named. However, our review showed that a single generic name used in the agreement in fact represented several intelligence services belonging to the government of the foreign state—in the Committee's view, a contravention of Ministerial Direction. We have subsequently been informed that the Service intends to request from the Minister appropriate corrections to the arrangement. The Committee will follow-up on the matter.

Our review showed that a single generic name used in the agreement in fact represented several intelligence services belonging to the government of the foreign state.

Collection of Foreign Intelligence

Report # 109

Foreign intelligence refers to the collection and analysis of information about the "capabilities, intentions or activities" of a foreign state. Under section 16 of the *CSIS Act*, the Service may, at the written request of the

Minister of Foreign Affairs and International Trade or the Minister of National Defence—and with the approval of the Solicitor General—collect foreign intelligence. The *Act* provides that the collection of information must take place in Canada, and cannot be directed at Canadian citizens, permanent residents or Canadian companies.

Methodology of the Audit

The Committee employs various methods to audit the collection and use of foreign intelligence:

- review Ministers’ “requests for assistance”;
- examine all information about Canadians retained by CSIS for national security purposes; and,
- scrutinize all CSIS requests for information to the Communications Security Establishment (CSE).¹⁹

Our goals are to,

- assess CSIS involvement in section 16 requests to ensure compliance with the Memorandum of Understanding, the *CSIS Act*, and directions from the Federal Court;
- determine whether the Service has met the various legal tests required to collect information under section 16 operations; and,
- in general terms, assess whether the Service’s cooperation with the CSE is in compliance with the *CSIS Act*.

Findings of the Committee

Ministerial Requests

For the period under review the Committee noted two significant developments regarding

Ministers’ requests for assistance. The first was a change in policy regarding the length of time requests would have effect before being renewed or cancelled. In our 1996-97 Annual Report, the Committee expressed concern about the existence of “stale-dated” requests up to five years old. During the year under review, the Committee was informed that a one-year validity limit had been imposed on all requests submitted to CSIS.

The second development was operational in nature. As in last year’s audit, when we reviewed the requests for assistance requiring Federal Court warrants we identified some which did not contain an explicit prohibition against the targeting of Canadians, nor did they specify the circumstances under which Canadians might be subjected to incidental interception. Both provisions are required by the 1987 Memorandum of Understanding between the Service and requesting government departments. CSIS has informed the Committee that it had again raised the matter with the Government department which subsequently advised that it would begin including the prohibition clause in its request letters.

Federal Court Decision

In September 1997, Madame Justice Donna McGillis of the Federal Court ruled on the “visitor’s clause” contained in a section 12 warrant being requested by the Service. In her opinion, this clause constituted an unlawful delegation of authority to CSIS.²⁰ During the most recent year under review, the Federal Court again took issue with the discretionary authority of CSIS senior managers, this time in regard to a section 16 warrant. The Service adjusted the warrant

accordingly, and has since undertaken a full review of the terms and conditions set out in section 16 warrants generally.

As we stated last year, the Committee regards the approval of warrants as the sole prerogative of the Federal Court. It is the Committee's responsibility to ensure that the Service rigorously observes conditions imposed on it by the Court. We will continue to monitor the Service's policies and operational practices in respect to its use of warrant powers.

Retention of Foreign Intelligence

The Committee identified two instances of inappropriate retention of information. Both concerned documents that had no obvious foreign or security intelligence relevance. The Committee brought these cases to the attention of the Service.

Section 16 Information and the Communications Security Establishment (CSE)

The information that CSE routinely gives to CSIS is "minimized" in order to comply with the prohibition on the collection of information on Canadian nationals and Canadian companies. The Service may, under special circumstances request identities if it believes the information is relevant to an ongoing section 12 ("threats to security") investigation. The Committee regularly scrutinizes these requests to CSE to ensure that they are appropriate and that they comply with existing law and policy.

Of the requests made during the current reporting period, three drew the Committee's attention because, in our view, the circum-

stances and subjects could not be considered threats to national security. For example, one case pertained to a straightforward criminal matter not within the Service's mandate.

Management, Retention and Disposition of Files

Files are the essential currency of intelligence gathering. Each CSIS investigation and every approved target requires the creation of a file, and a system for making the information in it available to those designated within the Service. Balanced against this information-gathering apparatus is the clear restriction on CSIS set out in the *CSIS Act*, that it shall collect information "to the extent that it is strictly necessary." The Committee closely monitors on an annual basis the operational files held by the Service.

In this year's Annual Report, in addition to the information about files which we regularly report on in this section, we also conducted a special review of files that were inadvertently overlooked by the CSIS file management system. A report on the results of our inquiries can be found on page 32.

File Disposition

CSIS files are held according to predetermined retention and disposal schedules that are negotiated with the National Archivist. These define how long the files are to be retained after Service employees cease using them. When this period expires, the National Archives Requirements Unit (NARU) in CSIS consults with Service operations staff on whether to keep the file, destroy it, or

It is the Committee's responsibility to ensure that the Service rigorously observes conditions imposed on it by the Court.

send it to the National Archives.

During fiscal year 1998-99, NARU reviewed 25,948 files which had come to its attention through the regular archival “Bring Forward” (BF) system. Of the files that NARU and the operational staff reviewed, 20,294 were destroyed and 5,618 were retained. CSIS informed us that 36 files were identified as having archival value. They were removed from the active file holdings and will be sent to National Archives according to the established schedules.

New File Statistics

We compiled file statistics for the past three fiscal years and noted several interesting trends:

- an increase in numbers of files on foreign nationals visiting Canada where there was a counter terrorism concern;
- the number of files on right wing extremists continues to decline slightly; and,
- security screening files overall show the expected minor fluctuations, however, the number of files devoted to immigration and refugee screening has increased over the last three fiscal years.

The Committee is cautious about drawing too much from these observations. A decrease or increase in the number of files does not, of itself, presage a change in threats to national security. Instead, the variations may reflect individuals’ membership or group preferences, or alternatively, a shift in focus on the part of the Service. We will analyse any significant trends in greater depth should they prove to be extended.

Section 2: Security Screening and Investigation of Complaints

A. Security Screening

In the context of the *CSIS Act*,²¹ the Service fulfills its security screening responsibilities in two different spheres: employment within the Federal Government when the position in question requires a security clearance, and security screenings for Canada's Immigration Program. Both activities involve the delivery of a service to other decision-makers in the form of security assessments.

For Federal employment, CSIS security assessments serve as the basis for determining an individual's suitability for access to classified information or assets. In immigration cases, Service assessments can be instrumental in Citizenship and Immigration Canada's decision to admit an individual into the country, and in the granting of permanent resident status or citizenship. More generally, intelligence gathered by the Service

forms the basis of immigration screening profiles used in processing applicants.

Security Screening Assessments in 1998-99

The number of government security screening assessments for this year was 31,885,²² with an average turnaround time of four days for a Level I, nine days for a Level II, and 111 days for a Level III. The Service also processed 26,364 requests under the Airport Restricted Access Area Clearance Program (ARAACP) which comes under the authority of Transport Canada. The Service provides its advice to its clients in the form of "briefs." According to statistics provided by CSIS, of the 58,249 assessments conducted in total, the Service issued no briefs recommending the denial of a clearance, and 13 "information" briefs.

Screening Arrangement with a Provincial Institution

The Solicitor General temporarily authorized the Service to conduct a limited number of checks of CSIS data banks concerning foreign specialists required to work for an agency

Security Clearance Decisions – Loyalty and Reliability

Decisions by federal departments to grant or deny security clearances are based primarily on the Service's recommendations. Reporting to the federal organization making the request, CSIS renders an opinion about the subject's "loyalty" to Canada, as well as the individual's "reliability" as it relates to loyalty. Government Security Policy stipulates that a person can be denied a security clearance if there are reasonable grounds to believe that,

- "As it relates to loyalty, the individual is engaged, or may engage, in activities that constitute a threat to the security of Canada within the meaning of the *CSIS Act*."
- "As it relates to reliability, because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties to persons living in oppressive or hostile countries, the individual may act or may be induced to act in a way that constitutes a 'threat to the security of Canada'; or they may disclose, may be induced to disclose or may cause to be disclosed in an unauthorized way, classified information."

of a provincial government. In such instances, the Service provides records checks and a security assessment but does not append a recommendation. The Service processed 70 requests resulting in one information brief.

Screening on Behalf of Foreign Agencies

The Service is authorized to enter into reciprocal arrangements with foreign agencies to provide security checks. These checks are provided on Canadians and other individuals who have resided in Canada. For the year under review, the Service processed 1,064 requests, 161 of which involved field investigations and resulted in 6 information briefs.

Immigration Security Screening Programs

The Service conducts security screening investigations and provides advice to the Minister of Citizenship and Immigration (CIC).

The Service's authority for immigration screening is derived from sections 14 and 15 of the *CSIS Act*. The nature of the Service's role²³ varies from information sharing (on matters concerning threats to the security of Canada) to assessments provided to CIC with respect to the inadmissibility classes of section 19 of the *Immigration Act*.

Immigration and Refugee Applications for Permanent Residence from Within Canada

CSIS has the sole responsibility for screening immigrants and refugees²⁴ who apply for permanent residence from within Canada. For the year under review, the Service received 30,945 requests for screening applicants under this program. CIC forwards the vast majority of these applications directly to CSIS for screening via an electronic data link from the CIC's Case Processing Centre (CPC) in Vegreville, Alberta. The average

SIRC's Role Regarding Complaints About CSIS Activities

The Review Committee, under the provisions of section 41 of the *CSIS Act*, must 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:

- the complainant must have first complained to the Director of CSIS, and have not received a response within a period of time that the Committee considers reasonable, (approximately thirty days) or the complainant must be dissatisfied with the Director's response; and
- 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*. These conditions do not diminish the Committee's ability to investigate cases and make findings and recommendations where individuals feel that they have not had their complaints answered satisfactorily by CSIS.

turn-around time for such applications is currently 11 days, 9 days for Canada-based electronic cases, and 96 days for paper cases.

Immigration and Refugee Applications for Permanent Residence from Outside Canada

Immigration and refugee applications for permanent residence that originate outside of Canada are managed by the Overseas Immigrant Screening Program. Under this Program, CSIS shares the responsibility for the security screening process with CIC officials abroad, usually the Immigration Program Managers.

As a general rule, CSIS only becomes involved in the immigration screening process if requested to do so by an Immigration Program Manager or upon receipt of adverse information about a case from established sources—a procedure that allows the Service to concentrate on the higher risk cases. The number of referrals to CSIS represents approximately 25 percent of the national volume. For the year under review, the Service received 21,576 requests for screening applicants under the Overseas Immigration Screening Program, 7,333 requests relating to applicants based in the United States, and 3,989 applicant files referred for consultation by CSIS Security Liaison Officers posted abroad.

Length of Time Taken for Security Screening

For the year under review, 50.3% of all immigration screening cases were completed in 43 days. Of the remaining 49.7%, the turn-around time was 92 days. Overall, 99.3%

of all immigration screening cases were completed in under one year.

Nature of the Service's Advice

During the period under review, the Service forwarded 128 briefs to CIC. Fifty-one of those were “information briefs” while the remaining 77 advised CIC that the person, in the view of the Service, was inadmissible to Canada on security grounds. Although the Committee has requested that the Service provide information on decisions that resulted from its advice, the Service has stated that because CIC considers a myriad of factors in deciding admissibility, it is not able to determine the impact of its advice on any individual decision.

Enforcement Information Index²⁵

EII, the CIC data bank, is designed to warn immigration officials abroad and alert officials at Canada’s points of entry about persons who may pose a security threat. Through this process, CSIS provides basic identifying data about individuals who could be the subject of enforcement action. During 1998-99, the Service supplied CIC with 132 names of known and suspected terrorists for addition to this index.

Point of Entry Alert System

Linked to the Enforcement Information Index, CSIS (through CIC and Revenue Canada) can issue a point-of-entry alert for any person of security concern whose arrival in Canada is thought to be imminent. The purpose is to allow CIC and Customs officials to determine that person’s admissibility. During 1998-99, the Service issued 15 point of entry alerts resulting in 8 interdictions. Three of the 15

The names of all applicants are sent to CSIS for cross-checking against names in the Security Screening Information System data base.

Security Screening in the Government of Canada

The Government Security Policy (GSP) stipulates two types of personnel screening: a reliability assessment and a security assessment. Reliability checks and security assessments are conditions of employment under the *Public Service Employment Act* (the “PSEA”).

Basic Reliability Status

Every department and agency of the Federal Government has the responsibility to decide the type of personnel screening it requires. These decisions are based on the sensitivity of the information and the nature of the assets to which access is sought. Reliability screening at the “minimum” level is required for those persons who are appointed or assigned to a position for six months or more in the Public Service, or for those persons who are under contract with the Federal Government for more than six months, and who have regular access to government premises. Those persons who are granted reliability status at the basic level are permitted access to only non-sensitive information (i.e., information which is not classified or designated).

Enhanced Reliability Status

Enhanced Reliability Status is required when the duties of a federal government position or contract require the person to have access to classified information or government assets, regardless of the duration of the assignment. Persons granted enhanced reliability status can access the designated information and assets on a “need-to-know” basis.

The federal departments and agencies are responsible for determining what checks are sufficient in regard to personal data, educational and professional qualifications, and employment history. Departments can also decide to conduct a criminal records name check (CRNC).

When conducting the reliability assessments, the Federal Government organizations are expected to make fair and objective evaluations that respect the rights of the individual. The GSP specifies that “individuals must be given an opportunity to explain adverse information before a decision is reached. Unless the information is exemptible under the *Privacy Act*, individuals must be given the reasons why they have been denied reliability status.”

Security Assessments

The *CSIS Act* defines a security assessment as an appraisal of a person’s loyalty to Canada and, so far as it relates thereto, the reliability of that individual. A “basic” or “enhanced” reliability status must be authorized by the government department or agency prior to requesting a security assessment. Even if a person has been administratively granted the reliability status, that individual must not be appointed to a position that requires access to classified information and assets, until the security clearance has been completed.

were interviewed and allowed into Canada. The Service has no information indicating that the others actually attempted to enter.

CSIS, Citizenship Applications and the Alert List

In 1997, CIC instituted a mail-in system whereby all applications for citizenship are processed by the Case Processing Centre (CPC) in Sydney, Nova Scotia. As part of the tracing procedures, the names of all applicants are sent to CSIS through electronic data transfers for cross-checking against names in the Security Screening Information System data base. There are presently a number of names on an Alert list comprised of individuals who had come to the attention of CSIS through TARC-approved investigations, and while not yet citizens, have received landed immigrant status.

The vast majority of citizenship applications are processed in an expeditious manner with

the rest requiring additional analysis by the Service before it sends a recommendation to Citizenship authorities. In fiscal year 1998-99, CSIS received a total of 159,939 names from CIC. Out of these, 36 cases had resulted in information briefs; none were recommendations for denial.

The Solicitor General has approved the deferral of two cases, while a third was in the process of being examined for a deferral.²⁶

Section B. Investigation of Complaints

As distinct from the Review Committee's function to audit and review the Service's intelligence activities, we have the additional task of investigating complaints from the public about any CSIS action. Three areas fall within the Committee's purview:

Table 3
Complaints (1 April 1998 to 31 March 1999)

	New Complaints	Carried Over from 1997-98	Closed in 1998-99	Carried to 1999-2000
CSIS Activities	53	3	37	19
Security Clearances	0	1	0	1
Immigration	0	0	0	0
Citizenship	0	1	0	1
Human Rights	1	0	1	0

- As a quasi-judicial tribunal the Committee is empowered to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees and contractors.
- The Committee can investigate reports made by Government Ministers about persons in relation to citizenship and immigration, certain human rights matters, and organized crime.
- As stipulated in the *CSIS Act*, the Review Committee can receive at any time a complaint lodged by a person “with respect to any act or thing done by the Service.”

Findings on 1998-99 Complaints “With Respect to Any Act or Thing”

During the 1998-99 fiscal year, we received 53 new complaints under section 41 of the *CSIS Act* (“any act or thing”). We also completed our investigation into a section 42 complaint carried over from 1996-97 but the report was not completed in time to be included in this year’s Annual Report. Our investigation of a Ministerial Report under sections 19 and 20 of the *Citizenship Act* was further delayed by legal proceedings.

We completed our investigation of a matter referred by the Canadian Human Rights Commission and with the agreement of the concerned parties and the assistance of an expert from the Commission, are attempting to determine whether the allegation (in this instance involving alleged discrimination) is justified.

CSIS Activities (Section 41): Immigration-Related Complaints

The year under review was marked by an increase in the number of complaints with respect to CSIS’ activities in immigration security screening.²⁷ The complaints were diverse in nature: the fact that applicants were not notified in advance about security screening interviews, the nature of particular interviews, the types of questions posed and the manner in which they were posed, the accuracy of the reporting following an interview, the kind of “cooperation”²⁸ complainants claimed was expected of them, the presumed content of the Service’s brief resulting from the interview (presumed, since the applicant does not see the brief), the length of time taken by the Service to provide its advice to Immigration authorities, the Service’s allegedly overly broad definition of the words “member” and “terrorist organization,” and allegations that attempts were made by

The Evolution of the Security Clearance Complaints Procedure

Until the *CSIS Act* was promulgated, not only were many individuals unaware that they had been denied a security clearance, but even those who were informed were often not told why their applications had been denied. Now, the law requires the Committee to give each individual who registers a complaint as much information about the circumstances giving rise to the denial of a security clearance as is consistent with the requirements of national security. The Committee must then examine all facts pertinent to the case, make a judgement as to the validity of the decision taken by the deputy head, and then make its recommendations to the Minister and the deputy head concerned.

CSIS to use the screening process in order to recruit individuals as sources.

The issues identified in the complaints were both complex and varied. While the Committee's inquiries into each complaint were not completed in time for the conclusions to be presented in this report, we have reached a number of conclusions about the obstacles we face in the process of reviewing the Service's role in immigration screening.

The first concerns the confusion that can occur because delays in any particular application can arise from several sources. It is often the case that applicants are without Counsel and are unfamiliar with the complaint procedures. In such cases, the Committee informs the individuals that they must first ascertain whether the delay is due to CSIS or to the Department of Citizenship and Immigration Canada.²⁹ If the former, the individual is required by statute to first submit a complaint to the Director of CSIS. Should the complainant receive an unsatisfactory response³⁰ or none at all, SIRC can then, and only then, become involved.

A second source of complexity which adds to the length of time required to inquire into immigration security screening matters is that the Service is not the mandated decision maker. The prime responsibility for the Immigration program lies with the Department of Citizenship and Immigration Canada, with the Service acting effectively in an advisory role. Since the Committee is empowered to investigate directly only CSIS activities, the determination of the impact of the Service's interviews and briefs on any particular

immigration application is time consuming and requires considerable investment of Committee resources.

Section 41: Complaints About CSIS Activities the Committee is Precluded From Investigating

We determined that two complaints received were not within our jurisdiction because the complainants were entitled to seek redress through other means set out in the *Public Service Staff Relations Act* and the *CSIS Act*. The individuals were so informed. Another case dealt with the complaints of a former Service employee. At the request of the Office of the Solicitor General the Committee reviewed the matter. The results of our inquiries are presented on page 30 of this report.

Complaints About CSIS Activities Determined to be Without Merit

The Committee reviewed twelve complaints about CSIS activities and in all cases determined that the Service was not involved in the alleged harassment. In an additional two cases, our investigations showed that allegations that CSIS has transmitted negative information to employers were unfounded.

Misdirected Complaints or Matters Sub Judice

Two complaints the Committee received were of a criminal nature and involved neither CSIS nor issues of national security. The Committee declined to take up either matter. In a third case, an individual complained to the Committee about the Service's decision not to meet with this individual who was then involved in a matter before the Courts. Upon

The year under review was marked by an increase in the number of complaints with respect to CSIS' activities in immigration security screening.

During the fiscal year under review the Government took no action to correct a situation the Committee stated some time ago should not be allowed to continue.

reviewing the issue the Committee determined that the Service's decision was appropriate.

Incomplete Assessment

The Committee concluded that the Service had acted in conformity with current policy when it informed a department of government that it was not in a position to provide an accurate and meaningful security assessment since the complainant in question had resided in Canada for less than twelve months.

We did note, however, that current policy did allow for special circumstances in which a deputy head of department could elect to grant the lowest level of clearance (Confidential) to an employee or contractor despite an incomplete Service assessment.

Security Clearance Complaints

Denial of a Security Clearance

As noted above, the Committee's investigation of a section 42 complaint was completed during the year under review. Our review included testimony from the Deputy Head of the department which had elected to deny the security clearance. The results of our inquiries were communicated to the various parties.

Unequal Access to "Right of Review"

In last year's Annual Report the Committee once again made strong note of a situation concerning the right to legal redress in the security screening system. Currently, employees falling under the jurisdiction of the *Aerodrome Security Regulations* and the

Aeronautics Act have only limited access to redress in the event they are denied a security clearance. During the fiscal year under review the Government took no action to correct a situation the Committee stated some time ago should not be allowed to continue.

Findings on 1998-99 Ministerial Reports

Citizenship Refusals

In the continuing matter regarding the citizenship application of Ernst Zündel, Mr. Zündel sought leave to appeal a 1997 decision by the Federal Court of Appeal which ruled that the Committee did have the right to investigate Mr. Zündel's case. The Supreme Court denied such leave on 30 April 1998.

Since the recommencement of our investigation, Counsel for Mr. Zündel applied for judicial review of a certain procedural notice of the investigating Member. Following a motion by the Attorney General of Canada to quash the application for review, Justice McKeown of the Federal Court on 18 June 1999 rejected Mr. Zündel's application. The Committee has since received notice of Mr. Zündel's intention to appeal this latest decision.

Ministerial Report Pursuant to the Immigration Act

The Committee received no Ministerial Reports of this type during 1998-99. A judicial review of a case involving a Ministerial Report received in 1996-97 is scheduled to be heard in August 1999 by the Federal Court.³¹

Federal Court of Appeal Decision

In a judgment delivered on 19 July 1999, the Federal Court of Appeal disposed of the judicial review of a decision the Committee had rendered in 1988. At that time, the Committee concluded that the subject individual was a person described in paragraph 19 (1) (g) of the *Immigration Act*: a person whom there are reasonable grounds to believe is likely to engage in acts of violence that would or might endanger the lives or safety of persons in Canada, or is likely to participate in the unlawful activities of an organization that is likely to engage in such acts.

The Committee had also recommended that a certificate be issued by the Governor in Council under subsection 40(1) of the *Immigration Act*, leading ultimately to the applicant's deportation from Canada. In a subsequent application for judicial review, the applicant challenged not only the conclusion of the Committee but its processes and procedures as well.

In its ruling on the judicial review, the Court concluded that the application should be dismissed substantially for the reasons given by the Supreme Court in *Chiarelli v. Canada (Minister of Employment and Immigration)*. The panel of Justices was not persuaded by the applicant's arguments that there were errors in previous decisions which had found that the Review Committee had "diligently and carefully considered the interest of the applicant in disclosure (of confidential documents)."

As in *Chiarelli* the Court stated that a finding had been made by the Committee that the applicant breached an essential condition of remaining in Canada and that the finding was in accordance with the principles of fundamental justice. The Court also concluded that the applicant's possible deportation was not due to a criminal conviction for a rather minor offence, but rather because he represented a danger to Canadians. The Court's ruling took pains to distinguish this case from that of *Al Yamani v. Canada (Solicitor General)* wherein a clause of the *Immigration Act* was determined to be in violation of the *Charter of Rights and Freedoms*. The Court was of the view that the Committee had not come to an unreasonable conclusion respecting the individual.

Canadian Human Rights Commission Referrals

During the year under review the Committee received one referral from the Canadian Human Rights Commission. Acting within the time constraints set out under the *Canadian Human Rights Act*, we conducted our investigation and reported to the Canadian Human Rights Commission, the Minister concerned, and the Director of CSIS.

We determined that the Minister's conclusion that providing certain information under the procedures of the particular human rights complaint at issue would reveal classified information was correct in fact and in law.

The Court concluded that the applicant's possible deportation was not due to a criminal conviction for a rather minor offence, but rather because he represented a danger to Canadians.

Section 3: CSIS Accountability Structure

The Service is an agency of the Government of Canada and as such, is accountable to Government, Parliament and the people of Canada. Because of the serious and potentially intrusive nature of CSIS activities, the mechanisms set out in law to give effect to that accountability are both rigorous and multi-dimensional; there are a number of independently managed systems inside and outside the Service for monitoring CSIS activities and ensuring that they accord with its mandate.

It is part of the Security Intelligence Review Committee's task (the Committee itself being part of the accountability structure) to assess and comment on the functioning of the systems that hold the Service responsible to government and Parliament.

A. Operation of CSIS Accountability Mechanisms

Ministerial Direction

Section 38(a)(ii) of the *CSIS Act*, directs the Committee to review Direction provided by the Solicitor General to the Service under subsection 6(2) of the *Act*. Ministerial Directions govern certain types of CSIS investigations in potentially sensitive areas, such as investigations on university campuses.

There are three elements to the Committee's analysis: an examination of instructions issued by the Service based on Ministerial Direction; a review of the manner in which Directions were implemented in specific

cases; and the identification of significant changes in the numbers of operations that require Ministerial approval. Our interest in all cases is to ensure that the relevant Ministerial Direction is adequately articulated and that there has been full compliance on the part of the Service.

There were two new Ministerial Directions issued during the period under review.

National Requirements for Security Intelligence 1998-99

National Requirements contain general direction from Cabinet as to where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis, and advisory responsibilities. For 1998-99, the National Requirements set out priorities for CSIS in eight areas: counter terrorism, counter intelligence, security screening, foreign intelligence support, foreign influenced activities, environmental scanning, intelligence liaison, and technology development.

New Areas of Interest

The last four areas represent a significant departure from past Directions which have typically identified only the first four. Specifically, the 1998-99 National Requirements direct the Service,

- to investigate *foreign influenced activities* detrimental to Canadian interests;³²
- to monitor, through *environmental scanning*, emerging threats to Canada that have the potential to become significant domestic problems, and to provide advice to Government accordingly;
- to maintain *intelligence liaison* relationships with its partners in an effort to persuade

former adversaries that their security needs can be met through liaison and cooperation rather than through the conduct of “hostile foreign intelligence activity in Canada.”; and,

- to anticipate the impact of new and emerging *technology developments* on its ability to effectively collect, process, and analyze intelligence.

Changed Emphasis in Existing Areas of Interest

In addition to these wholly new areas of interest, the 1998-99 *National Requirements* modified several existing ones. With respect to transnational criminal activity, the Minister wrote that CSIS should focus on the “increased health and welfare costs caused by the consumption and trade of illegal drugs as well as erosion of the tax base due to unreported illegal business transactions.” In the Committee’s view, this change in emphasis appears to broaden the already wide scope of CSIS activities in this sector and would seem to add to the ongoing debate about the Service’s role in combating international organized crime. (See “Review of Transnational Criminal Activity” p. 5)

Finally, under the category of counter intelligence, the Minister also instructed the Service “to monitor and investigate attacks on information operations in so far as they pose a threat to the security of Canada.”

Rules Governing the Use of Sources

In late 1998, the Minister issued an addendum to the October 1986 Ministerial Direction on the use of government officials as confidential sources of information and assistance.

The addendum extended the rules governing the recruitment of Federal Government employees as CSIS sources to all employees of Parliament and Parliamentarians.

The 1986 rules applying to Federal employees require the Service to take certain actions before recruiting an employee as a source. They also make provision for the Minister to waive that requirement if CSIS convinces him or her of an operational necessity to do so. Since neither staff of the Parliament of Canada nor Parliamentarians are Federal employees, the new Direction instead requires that in each instance CSIS must consult the Solicitor General before recruitment. The Committee will monitor the implementation of the new policy and the Service’s adherence to the protocol which governs it.

Changes in Service Operational Policies and Instructions to Officers

The CSIS *Operational Policy Manual*, derived in part from the Service’s interpretation of Ministerial Direction, is intended as a guide and operational framework for CSIS employees. The Committee examines changes to the *Operational Policy Manual* as if they were changes to Ministerial Direction, and regards the manual as a useful tool in assisting our reviews of CSIS investigations. Operational policies, some of which are sensitive and potentially intrusive, must comply with Ministerial Direction, the *CSIS Act*, the *Canadian Human Rights Act* and other relevant legislation.

In fiscal year 1998-99, the Service produced one new policy and made several significant amendments to existing policies.

The Minister also instructed the Service “to monitor and investigate attacks on information operations in so far as they pose a threat to the security of Canada.”

The Committee examines changes to the *Operational Policy Manual* as if they were changes to Ministerial Direction.

Advice on Threats

Government Security Policy requires Government departments and agencies to safeguard their classified information and assets, and to conduct the Threat and Risk Assessments necessary to that end. The new CSIS policy outlines the Service's responsibilities in providing, upon request, advice to client departments and agencies on any known, suspected or potential threats (as defined under section 2 of the *CSIS Act*) directed against clients' assets.

Physical Surveillance

CSIS made significant amendments to the operational policy applying to physical surveillance. The revised sections are intended to make policy more explicit and intelligible, clearly outlining the principles, responsibilities, procedures, and approval mechanisms necessary for all physical surveillance operations undertaken by the Service.

Other Changes

We noted two other amendments to existing policies. The first pertained to the collection of foreign intelligence under section 16 of the *CSIS Act*, and addressed the requirements to separately report information if the Service retains information about threats to the security of Canada as provided under section 12 of the *Act*. The second amended the rules governing certain Service practices.

Disclosure of Information in the Public and in the National Interest

In the Public Interest

Section 19 of the *CSIS Act* prohibits the Service from releasing information collected

in its investigations, except in specific circumstances. Under one circumstance, explicitly referred to in 19(2)(d) of the *Act*, the Minister can authorize the Service to disclose information in the "public interest." The *Act* compels the Director of CSIS to submit a report to the Committee regarding all "public interest" disclosures.

There had been no releases under this section of the *CSIS Act* until 1998-99, when all Federal Government departments and agencies were asked to facilitate the RCMP Public Complaints Commission (PCC) inquiry into police conduct at APEC³³ by providing all relevant information in their possession. CSIS identified 66 documents and one video³⁴ as possibly having some relevance. The Director sought and obtained the Solicitor General's authority to permit PCC counsel to view the 67 items.

The PCC counsel's review identified 17 items that were of interest. In July 1998, the Minister authorized the release of 14 of them; the remaining three were not released on national security grounds.

The *CSIS Act*, requires the Director to provide us with a report of all disclosures in the public interest. On 10 June 1999—almost one year after the disclosures—we received the Director's formal report from CSIS.

We confirmed that the Minister had indeed authorized the release of the 14 items, and concurred that the public interest in each case clearly outweighed the privacy considerations arising from that disclosure. However, we found the delay in providing the Committee

with the report excessive. We have so advised the Director of CSIS.

In the National Interest

Under the Service's interpretation of its mandate, it holds that, acting as the Minister's agent CSIS can disclose information in the "national interest." In such circumstances, the Solicitor General would determine whether the disclosure of operational information was in fact in the national interest, whereupon he would direct CSIS to release the information to persons or agencies outside government. CSIS policy stipulates that the Committee be informed whenever such disclosures take place. There were none in 1998-99.

Governor in Council Regulations and Appointments

Under section 8(4) of the *CSIS Act*, the Governor in Council may make regulations concerning the powers of the Director of CSIS, appointments and other personnel matters. No such regulations were issued in 1997-98.

Annual Report of the Director of CSIS

The CSIS Director's Annual Report to the Solicitor General comments in some detail on the Service's operational activities for the preceding fiscal year. Among the key functions of the Committee is the review of this report.

Last year, the Committee did not receive the Director's report in time for inclusion in our 1997-98 audit report. Therefore, we present the review here.

Director's Report for 1997-98

From the Committee's perspective, the salient points of the Director's Annual Report of 1997-98 were the following:

- *Public safety*
Public safety remained the highest priority for the Service and represented 60 percent of the more than one thousand active investigations in the period April 1997 through March 1998. Terrorism linked to Asian and Middle Eastern conflicts was a major focus of the Service's efforts.

CSIS Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada" which it is specifically charged to investigate include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state..." [section 2(c), *CSIS Act*]

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in the denial of citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

Public safety remained the highest priority for the Service and represented 60 percent of the more than one thousand active investigations.

- *National security*

In 1997-98, CSIS initiated a program to understand and evaluate the threat posed to national security by foreign agents who could exploit vulnerabilities in Canada's computer and telecommunications networks.

- *Security screening*

In 1997-98, the number of requests received by the Security Screening Branch from domestic and foreign agencies increased dramatically and during the last 3 years has almost tripled.³⁵

- *Foreign intelligence*

The Service effectively increased its output of foreign intelligence reports for other Federal Government departments in fiscal year 1997-98.

- *Foreign liaison*

In 1997-98, CSIS developed and presented its first training course for foreign intelligence services.

- *Funding*

The funding of a CSIS technical development program was terminated in 1997-98. The Director stated that given ongoing developments in communications technology, the absence of such a program would erode the quality of advice the Service could give to government in the future.

SIRC Comments

In the Committee's view, the Director's Annual Report for 1997-98 was a good overview of CSIS activities, and in contrast

with previous reports, provided more details about Service investigations. However, the Report failed to address some issues we regard as important:

- The report was silent on the threat posed by the use of chemical and biological weapons for terrorist purposes. We believe CSIS should report its findings on this threat to public safety.
- Whereas a Ministerial Direction specifically mentioned the importance of investigating a certain form of espionage, as measured by the Director's report, this area did not appear to be a high priority for the Service.
- The report does not address the material increase in the number of certain targeting authorizations conducted at the most intrusive level. We believe this is important information which should be conveyed to the Solicitor General.
- The report does not devote specific attention to joint operations with foreign services. The Committee is of the view that such operations are directly relevant to issues of Ministerial authority and thus merit appropriate attention from the Director.
- We saw no discussion of various recent legal judgements and their actual or potential impact on CSIS operations. For example, the report does not mention the Federal Court's decision on the use of the "visitor's clause" (also known as the McGillis decision, see p. 47 of our 1997-98 report) or its rejection of two Service applications for warrants in 1997-98.

Certificates of the Inspector General

The Inspector General of CSIS reports to the Solicitor General and functions effectively as his internal auditor of CSIS, reviewing the operational activities of the Service and monitoring compliance with its policies. Every year the Inspector General must submit to the Minister a Certificate stating the “extent to which (he or she) is satisfied,” with the Director’s report on the operational activities of the Service and informing the Minister of any instances of CSIS having failed to comply with the *Act* or Ministerial Direction, or that involved an unreasonable or unnecessary exercise of powers. The Minister sends a copy of the Certificate to the Security Intelligence Review Committee.

The Inspector General’s Certificates for 1996 and 1997 were briefly reviewed in last year’s Annual Report. We commented that some of the issues raised in the Certificates were complex and required more time for study than was available to us before the deadline for the 1997-1998 Annual Report. The most complex of these matters—“issue-based” targeting—the Committee decided was of such importance as to warrant special consideration. The results of our review can be found on page 33 of this report.

The other issues addressed by the Inspector General in the 1996 and 1997 Certificates were technically complex but did not involve the general philosophy or principles associated with targeting or investigating threats to the security of Canada.

The Inspector General noted several areas where, in his view, the letter of the law as

specified in Ministerial Direction had not been followed in a precise or rigorous enough manner. Though we have not investigated the particular cases cited by the Inspector General, we certainly agree with the proposition that the rationale for targeting any person or any other action involving CSIS’ extensive powers should be fully documented in CSIS files. We also agree that Ministerial Direction should be followed both in letter and in spirit. Where this turns out to be impractical or administratively very cumbersome, CSIS should attempt to convince the Minister that his or her Direction could reasonably be amended.

SIRC has not received a 1998 Certificate from the Inspector General because the position was vacant from June 1998 until September this year.

Unlawful Conduct

Under section 20(2) of the *CSIS Act*, the Director of CSIS is to submit a report to the Minister when, in his opinion, a CSIS employee may have acted unlawfully in the performance of his or her duties and functions. The Minister, in turn, must send the report with his comments to the Attorney General of Canada and to the Committee.

In 1998-99, we received one report of possible unlawful conduct by an employee of CSIS. No decision has been received yet from the Attorney General of Canada concerning this case.

In last year’s report, we commented on two cases of unlawful conduct dating back to 1989 and 1990 which remained unresolved.

We agree that the rationale for targeting any person or any other action involving CSIS’ extensive powers should be fully documented.

We have since been informed that the cases were brought to conclusion with no charges being laid by the Attorney General of Canada against the employees in question.

We also commented on another case of unlawful conduct dating back to 1997. Following a criminal investigation, CSIS elected to conduct its own internal inquiry. The Committee will comment on the matter upon its conclusion.

SIRC Consultations and Inquiries

The Committee is a key part of the CSIS accountability structure. In 1998-99 we undertook specific activities in this respect in the following areas:

Tracking and Timing of Formal Inquiries

In our review function, we send questions to CSIS to request information and/or documents about its activities. In the 1998-99 fiscal year (April 1, 1998 to March 31, 1999) we directed 126 formal inquiries to the Service. The average time CSIS took to respond to a formal inquiry was 38.5 days (essentially unchanged from last year)—a figure that does not include questions arising out of complaint cases.

In addition to formal questions, the Committee makes informal requests of CSIS. In all such cases for the year under review, the Service responded expeditiously to what were sometimes urgent queries.

Briefings

At its monthly meetings, the Chair and Committee Members meet with government officials to keep open the lines of communication

and stay abreast of new developments. When meetings of the Review Committee are held outside of Ottawa, Members visit CSIS regional offices. The Committee met with senior CSIS regional managers in Montreal in September 1998, in Vancouver in February 1999, and in Toronto in April 1999. The balance of the Committee's meetings were held in Ottawa.

SIRC Activities Additional to CSIS Review

In October 1998, Committee Members met with the Director General of the Security and Intelligence Bureau and the Director of Foreign Intelligence Division from the Department of Foreign Affairs and International Trade. The Committee met with the Communications Security Establishment Commissioner in November 1998.

In November 1998, at the invitation of the Swedish Government, the Chair met with the President of Svea Court of Appeal in Stockholm, and with members of the Commission of Inquiry into the Swedish Intelligence Service. Also, the Chair and the Executive Director travelled to the United Kingdom in November 1998 to meet with the Intelligence and Security Coordinator, the UK Parliament's Intelligence and Security Committee, and the Deputy Head of MI5.

The Committee also met with the Solicitor General in May 1999.

At the end of June 1999, the Committee hosted an international conference of heads of intelligence review agencies. The conference is discussed on page 67.

Special Reports

Under section 54 of the Act, the Committee can be asked by the Minister to report to him or her on any matter relating to the performance and functions of the Service. In 1998-99, we submitted one such study to the Minister entitled, *Allegations by a Former CSIS Employee*. Details can be found on page 30.

B. Inside the Security Intelligence Review Committee

On 18 June 1999, the Prime Minister of Canada announced the appointments of the Honourable Ray Speaker, P.C., and the Honourable Frank McKenna, P.C. to SIRC. These appointments mark the first time since November 1997 that the Committee has had its full complement of Members.

On 29 July 1999, the Solicitor General of Canada announced the appointment of Maurice Archdeacon as the Inspector General of CSIS. Mr. Archdeacon had been SIRC's Executive Director since its establishment in 1985.

Intelligence Review Agencies

Conference

In June 1999 SIRC hosted an international conference in Ottawa to mark its 15th anniversary. The conference, "Review and Oversight in the New Millennium: Challenges of a Multipolar World" was attended by current and former SIRC Members, and the heads of review agencies from Canada, Australia, New Zealand, the United Kingdom, Belgium, South Africa, and the United States.

This was the second conference of its type, the first having been held in Canberra, Australia in November 1997. The Ottawa meeting provided an opportunity for the

Table 4
SIRC Budget 1998-99*

	1998-99	1997-98
Personnel	925,000	831,000
Goods and Services	589,000	575,000
Total Operating Expenses	1,514,000	1,406,000

Source: 1999-2000 Estimates, Part III, Section IV.

* Includes supplementary budget

delegates to address the challenges encountered in their respective jurisdictions, and to share problem-solving strategies.

The two-day conference was comprised of a series of working sessions, and other planned activities. For example, Members of the Parliamentary Standing Committee on Justice and Human Rights and Members of the Special Senate Committee on Counter Terrorism discussed legislators' relationships with review bodies, and invited journalists specializing in security intelligence issues participated in a working session on "Relationships with the Media."

The participants included Claude Bisson, Commissioner of the Communications Security Establishment; Senator William Kelly, Chair of the Senate Special Committee on Security and Intelligence; Ward Elcock, Director of CSIS; Jacques Saada, M.P., Parliamentary Secretary to the Solicitor General of Canada, and a Member of the Parliamentary Standing Committee on Justice and Human Rights; John Maloney, M.P., Chair of the Standing Committee on Justice and Human Rights; and other Members of that Committee: Derek Lee, M.P., and Ivan Grosse, M.P.

Symposia

In January 1999, the Committee's former Project Leader was a guest speaker at a conference organized by the Comité permanent de contrôle des Services de Renseignement in Brussels. Research Staff participated in the conference and the annual general meeting of the Canadian Association for Security and Intelligence Studies (CASIS) in Ottawa in June 1998.

Accounting to Parliament

On September 1, 1998, the Hon. Paule Gauthier, SIRC Chair, the Hon. Bob Rae, Committee Member, SIRC's Executive Director and Deputy Executive Director appeared before the Special Senate Committee on Security and Intelligence to answer questions about the role and functions of the Review Committee.

Staying in Touch with Canadians

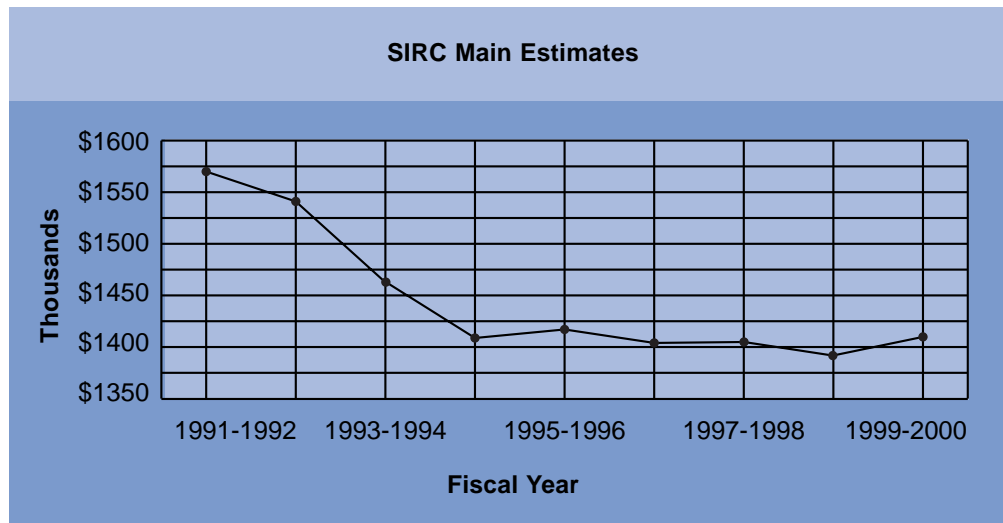
SIRC on the Internet

Since its debut on the Internet in October 1996, the SIRC web site (www.sirc-csars.gc.ca) has received almost 600,000 visits. In the Spring of 1999, the Committee used its site and the Public Service Commission site to advertise job competitions for two research positions; we received almost four hundred applications.

All SIRC Annual Reports, dating back to 1984-85 when the Committee was established, are now accessible through the web site. The list of Committee studies has been updated and we have added hot links to other sites of interest. The site also sets out procedures for filing complaints about CSIS activities and the denial of security clearances, as described in sections 41 and 42 of the *CSIS Act*.

Impact of Budget Reductions

Government-wide budget reductions continue to have an impact on the Committee's research functions. The investigation of complaints is the most expensive area of discretionary spending, and must, therefore, bear the brunt of recent budget cuts. To deal with the reductions, the Committee continues to rely



on the expertise of our staff Legal Counsel rather than retaining outside lawyers. Pre-hearing meetings also help the Committee make better use of resources by paving the way for hearings that are more focused and efficient. At the same time, the Committee is determined both to avoid increasing the time required to handle complaints and to maintain the high quality of its reports. The Committee believes the steps outlined above will allow SIRC to continue to improve its performance while meeting its responsibilities to Parliament and the public at lower cost.

The Committee has too small a staff to undertake “year 2000” information technology research on its own and thus has engaged outside specialists for this vital work. It is the Committee’s policy to remain informed about advances in information technology so as to continue the steady increase in staff productivity seen over the last six years.

Personnel

The Committee has a staff of fourteen: an executive director, a counsel/senior complaints officer to handle complaints and ministerial reports, a deputy executive director, a director of research, a project leader and five research officers (one of whom is responsible for liaison with the media), an administrative officer who is also the Committee registrar for hearings, and an administrative support staff of three to handle sensitive and highly-classified material using special security procedures.

At its monthly meetings, the members of the Committee decide formally on the research and other activities they wish to pursue, and set priorities for the staff. Management of the day-to-day operations is delegated to the Executive Director with direction when necessary from the Chair in her role as the Chief Executive Officer of the organization.

Glossary

APEC	Asia Pacific Economic Cooperation Conference
ARAACP	Airport Restricted Access Area Clearance Program
BF	Bring Forward Date
CAUT	Canadian Association of University Teachers
CI	Counter Intelligence
CIC	Citizenship and Immigration Canada
COMMITTEE	Security Intelligence Review Committee (SIRC)
CPC	Case Processing Centre
CRNC	Criminal Records Name Check
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism
Director	The Director of CSIS
EII	Enforcement Information Index
EXIPC	Executive Intelligence Production Committee
FLV	Foreign Liaison & Visits Branch
GSP	Government Security Policy
IAB	Intelligence Assessments Branch
IAC	Intelligence Assessment Committee

IAT	Independent Advisory Team
IO	Intelligence Officer
NARU	National Archives Requirements Unit
OPS	<i>Operational Policy Manual</i>
PSEA	<i>Public Service Employment Act</i>
RAP	Analysis and Production Branch
RCMP	Royal Canadian Mounted Police
PCC	Public Complaints Commission (RCMP)
RTA	Request for Targeting Authority
SERVICE	Canadian Security Intelligence Service (CSIS)
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer
TARC	Target Approval and Review Committee

SIRC Reports and Studies

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

1. *Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues*, (SECRET) * (86/87-01)
2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service*, (SECRET) * (86/87-02)
3. *The Security and Intelligence Network in the Government of Canada: A Description*, (SECRET) * (86/87-03)
4. *Ottawa Airport Security Alert*, (SECRET) * (86/87-05)
5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions*, (SECRET) * (87/88-01)
6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS*, (UNCLASSIFIED) * (86/87-04)
7. *Counter-Subversion: SIRC Staff Report*, (SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening*, (SECRET) * (87/88-03)
9. *Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement*, (PUBLIC VERSION) * (87/88-04)
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process*, (SECRET) * (88/89-01)
11. *SIRC Review of the Counter-Terrorism Program in the CSIS*, (TOP SECRET) * (88/89-02)
12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS*, (SECRET) * (89/90-02)
13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement*, (SECRET) * (89/90-03)

14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information*, (SECRET) (89/90-04)
15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information*, (SECRET) * (89/90-05)
16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons*, (UNCLASSIFIED) (89/90-06)
17. *SIRC Report on the Innu Interview and the Native Extremism Investigation*, (SECRET) * (89/90-07)
18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988*, (SECRET) * (89/90-01)
19. *A Review of the Counter-Intelligence Program in the CSIS*, (TOP SECRET) * (89/90-08)
20. *Domestic Exchanges of Information*, (SECRET) * (90/91-03)
21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue*, (SECRET) (90/91-06)
22. *Regional Studies (six studies relating to one region)*, (TOP SECRET) (90/91-04)
23. *Study of CSIS' Policy Branch*, (CONFIDENTIAL) (90/91-09)
24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets*, (TOP SECRET) (90/91-05)
25. *Release of Information to Foreign Agencies*, (TOP SECRET) * (90/91-02)
26. *CSIS Activities Regarding Native Canadians—A SIRC Review*, (SECRET) * (90/91-07)
27. *Security Investigations on University Campuses*, (TOP SECRET) * (90/91-01)
28. *Report on Multiple Targeting*, (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq*, (SECRET) (91/92-01)

30. *Report on Al Mashat's Immigration to Canada*, (SECRET) * (91/92-02)
31. *East Bloc Investigations*, (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions*, (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians*, (SECRET) (91/92- 03)
34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) * (91/92-04)
35. *Victor Ostrovsky*, (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case*, (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study*, (SECRET) * (91/92-07)
38. *The Attack on the Iranian Embassy in Ottawa*, (TOP SECRET) * (92/93-01)
39. *"STUDYNT" The Second CSIS Internal Security Case*, (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review*, (TOP SECRET) * (90/91-13)
41. *CSIS Activities with respect to Citizenship Security Screening*, (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations*, (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews*, (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal*, (TOP SECRET) * (90/91-10)
45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review*, (TOP SECRET) * (91/92-14)
46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)*, (TOP SECRET) * (90/91-11)
47. *The Assault on Dr. Hassan Al-Turabi*, (SECRET) (92/93-07)
48. *Domestic Exchanges of Information (A SIRC Review—1991/92)*, (SECRET) (91/92-16)

49. *Prairie Region Audit*, (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa*, (SECRET) (CT 93-06)
51. *Regional Audit*, (TOP SECRET)
52. *A SIRC Review of CSIS' SLO Posts (London & Paris)*, (SECRET) (91/92-11)
53. *The Asian Homeland Conflict*, (SECRET) (CT 93-03)
54. *Intelligence - Source Confidentiality*, (TOP SECRET) (CI 93-03)
55. *Domestic Investigations (1)*, (SECRET) (CT 93-02)
56. *Domestic Investigations (2)*, (TOP SECRET) (CT 93-04)
57. *Middle East Movements*, (SECRET) (CT 93-01)
58. *A Review of CSIS' SLO Posts (1992-93)*, (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats*, (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests*, (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information*, (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada*, (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 93-11)
64. *Sources in Government*, (TOP SECRET) (CI 93-09)
65. *Regional Audit*, (TOP SECRET) (CI 93-02)
66. *The Proliferation Threat*, (SECRET) (CT 93-07)
67. *The Heritage Front Affair. Report to the Solicitor General of Canada*, (SECRET) * (CT 94-02)
68. *A Review of CSIS' SLO Posts (1993-94)*, (SECRET) (CT 93-09)

69. *Domestic Exchanges of Information (A SIRC Review 1993-94)*, (SECRET) (CI 93-08)
70. *The Proliferation Threat - Case Examination*, (SECRET) (CT 94-04)
71. *Community Interviews*, (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation*, (TOP SECRET) * (CI 93-07)
73. *Potential for Political Violence in a Region*, (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS' SLO Posts (1994-95)*, (SECRET) (CT 95-01)
75. *Regional Audit*, (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government*, (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada*, (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services*, (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994-95)*, (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial*, (SECRET) (CT 95-04)
82. *CSIS and a "Walk-In"*, (TOP SECRET) (CI 95-04)
83. *A Review of a CSIS Investigation Relating to a Foreign State*, (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 95-05)
85. *Regional Audit*, (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats*, (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information*, (SECRET) (CI 95-01)
88. *Homeland Conflict*, (TOP SECRET) (CT 96-01)

89. *Regional Audit*, (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources*, (TOP SECRET) (CI 96-03)
91. *Economic Espionage I*, (SECRET) (CI 96-02)
92. *Economic Espionage II*, (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-97*, (TOP SECRET) (CI 96-04)
94. *Urban Political Violence*, (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information (1996-97)*, (SECRET) (SIRC 1997-02)
96. *Foreign Conflict, Part I*, (SECRET) (SIRC 1997-03)
97. *Regional Audit*, (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies*, (TOP SECRET) (SIRC 1997-05)
99. *Spy Case*, (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations (3)*, (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation with the RCMP, Part I*, (SECRET) * (SIRC 1998-04)
102. *Source Review*, (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case*, (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest*, (TOP SECRET) (SIRC 1998-08)
105. *CSIS' Role in Immigration Security Screening*, (SECRET) (CT 95-06)
106. *Un conflit étranger - deuxième partie* (TOP SECRET) (SIRC Study 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC Study 1998-01)
108. *CSIS Cooperation with the RCMP - Part II* (SECRET) * (SIRC Study 1998-04)

- 109. *Audit of Section 16 Investigations & Foreign Intelligence 1997-98* (TOP SECRET) (SIRC Study 1998-07)
- 110. *Review of Intelligence Production* (SECRET) (SIRC Study 1998-09)
- 111. *Regional Audit* (TOP SECRET) (SIRC Study 1998-10)
- 112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC Study 1998-11)
- 113. *Allegations by a Former CSIS Employee*, (TOP SECRET) * (SIRC 1998-12)
- 114. *CSIS Investigations on University Campuses* (SECRET) (SIRC Study 1998-14)
- 115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC Study 1998-15)
- 116. *Files* (TOP SECRET) (SIRC Study 1998-16)

List of Recommendations and Major Issues

Statement from the Review Committee –

Recommendation for a Comprehensive Review of Canada's Security Intelligence Systems

In any democratic society security intelligence activities are among the most serious a government can undertake. They warrant the constant and meticulous attention of all who cherish democratic values and civil discourse in a turbulent and dangerous world.

The current security intelligence apparatus was designed twenty years ago, and last examined as a whole in 1990. The Members of SIRC believe that it is time, therefore, for a thorough Government-wide review of all of the nation's intelligence systems and organizations.

The mechanisms of such a comprehensive examination are for Government to choose, however, we would urge that the review be as open as law and prudence permit, and that all interested parties, individuals, and groups, be encouraged to participate.

Review of Transnational Criminal Activity

In the Committee's view, the question of whether CSIS' mandate permits its involvement in the investigation of transnational criminal activity remains open at the present time. There is a larger public policy question to be addressed by Government. Currently, CSIS is following Ministerial instructions to deal with issues of international crime, however, our reviews pointed to a number of problems in regard to the Service taking on the task. Given the importance of the matter, we would urge the Government to consolidate and clarify its intentions on how to address this growing array of threats to Canada.

The threshold for CSIS intervention ought to be clearly articulated: Service participation should be contingent on the criminal activity being of such seriousness and scope as to represent a genuine threat to the strategic, social, economic, and national security interests of Canada. The Service should not become involved in the investigation of criminal activities best left to law enforcement agencies.

Should CSIS continue to remain involved in the area, the Committee recommends that,

it develop a clear operational policy in all its aspects for investigating transnational criminal activity. Such policy should include the requirement to assess each case whenever consideration is given to initiating an investigation under an issue-based targeting authority; and,

it implement a program of specialized training in the key areas of transnational crime in order that the objective of providing strategic intelligence to the government on major international criminal activities can be fully realized.

Review of Intelligence Production

While the Committee acknowledges that as an organizational reality clients in Counter Intelligence and Counter Terrorism will continue to influence much of what RAP does, we remain convinced that the Service should continue active efforts to accommodate its external partners, and that it is possible to seek a better balance without penalty to internal operations.

There is, we believe, a similar lack of balance in the area of strategic analysis. Our discussions with both RAP's internal and external clients evinced the clear need for more and better long-range, strategic analysis.

In order to redress these shortcomings renewed direction from CSIS senior management is required. To this end, the Committee has two recommendations:

The reinvigoration of an apparatus that has become defunct in recent years — the Executive Intelligence Production Committee (EXIPC).

The articulation by CSIS of a specific plan to meet the clear requirement of both internal and external clients for more strategic analysis.

Our review identified a troubling form of professional segregation within the Branch. RAP staff who are not classified as intelligence officers (IOs) are treated differently in the areas of salary, training, and career advancement.

In order to address these issues, the Committee recommends,

that the Service develop quality control guidelines and protocols for its written product, and devise methodologies for checking the veracity of information on which reports are based;

that CSIS implement a comprehensive career plan encompassing all RAP officers, IOs, and non-IOs alike; and,

that a reasonable proportion of supervisory positions within the RAP establishment be designated for officers in the non-IO category.

CSIS Investigations on University Campuses

As a general rule, CSIS officers rely on relevant sections of the *CSIS Operational Policy Manual* which are derived from Ministerial Direction. Therefore, an examination of the Service's interpretation of Ministerial Directions, as expressed in its policy manual, was an important part of our review. The Committee identified some potential problems:

- in instances where the Minister's approval is still needed, the policy manual excluded the requirement set out in Ministerial Direction that the Service provide an explanation to the Minister of how the proposed operation would affect the rights and freedoms of the subjects of the investigation and others associated with the institution;
- a term for a particular type of investigative activity has been subject to too broad and varied an interpretation;
- the policy contained no references to the seminal 1963 Pearson-Laskin Accord; and,
- the policy permits CSIS officers, without Ministerial approval, to go on campus to collect information for security screening purposes and for other mandated enquiries; such enquiries not being adequately defined.

Two recommendations emerged from our study of CSIS campus operations:

First, when requesting authorization from the Minister, the Service should be required to explain how a particular investigation will impact on the rights and freedoms of persons who are subjects of the investigation as well as those persons associated with the institution concerned.

Second, the *CSIS Operational Policy Manual* should include in the authorities section explicit reference to the 1971 Record of Cabinet Decision articulating the general principles of the Pearson-Laskin Accord on campus investigations.

CSIS Cooperation with the RCMP - Part II

While there continues to be some residual friction in two regions between Service officers and their RCMP counterparts over especially difficult cases that arose in the recent past, the Committee believes that these have created no ongoing impairment to operational effectiveness. With the exception of two ongoing concerns—RCMP use of CSIS intelligence in criminal proceedings, and CSIS responsibility in the area of transnational crime—the CSIS-RCMP relationship can be characterized as one of genuine and fruitful cooperation.

CSIS Liaison with Foreign Agencies

Human Rights

The Committee believes that all possible care should be taken to make sure that the Service's exchanges of information are not used to assist in the violation of human rights. In order to ensure that the dissemination of information is tightly controlled, Security Liaison Officers (SLO) must make available to the rest of CSIS timely and accurate information about an agency's human rights record, as well as its propensity to pass information onto third parties without authorization.

Comprehensive Review of All Foreign Arrangements

Fully one-half of the Service's 215 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS and, of these, many pre-dated even the 1982 Ministerial Direction. The Review Committee is concerned at the delay in an anticipated release of new Ministerial Direction since our earlier recommendation that CSIS systematically reexamine all foreign arrangements is contingent on new Direction. We strongly urge the Ministry to replace the 1982 Ministerial Direction with one that reflects the Government's experience with the administration of foreign liaison arrangements to date, and that is consistent with the *CSIS Act*.

A General Finding

The Committee's periodic reviews of the Service's overseas liaison activities encompass all the many difficulties associated with work in foreign posts. SLOs sometimes face environments which are personally and professionally challenging. In general, the SLOs in the two posts reviewed demonstrated initiative, employed good judgement, and the Service exercised commendable restraint in deciding what information would be shared with its foreign partners.

Allegations by a Former CSIS Employee

In July 1998, the then Solicitor General, the Honourable Andy Scott, advised the Committee of certain allegations against CSIS by a former employee of the Service. In accordance with section 54 of the *CSIS Act*, the Minister asked us to report on the matter, reviewing the allegations and detailing the facts, if any, on which the allegations were based. The Committee concluded that all of the allegations were unfounded and so reported to the Minister.

Overlooked Files

In early 1998, while conducting file reviews at CSIS Headquarters, the Committee came across files that were opened by the RCMP Security Service, and which had been overlooked during the Service's major review in 1990 of all of the files inherited from the RCMP. Our review of the files revealed that the misplaced files were due to "administrative oversight": the files had inexplicably not been assigned a Bring Forward (BF) date during the Service's 1990 major review.

In general, although we found CSIS' file review process to be sound, we did find problems in the Service's implementation of that process. With the aim of rectifying these issues, the Committee made three recommendations:

First, that the *File Review and Disposition Guidelines* be updated to reflect the Service's present policy and operational requirements.

Second, that the operational units be required to comply with National Archives Requirements Unit (NARU) deadlines for disposal decisions, and that NARU establish an effective follow-up process.

Third, that analysts in NARU and the operational desks provide detailed rationales for their decisions to retain files, citing the applicable criteria listed in the Schedules and the Service's interest pursuant to the *CSIS Act*.

Complaint Case Histories

This section describes complaint cases submitted to the Review Committee during the past year on which decisions have been reached. Not addressed are complaints that were subject to administrative review, were misdirected, were outside the Committee's mandate, or on which decisions have not yet been rendered.

Both cases described below arose from Service activities in support of the Immigration Program and were lodged under section 41 of the *CSIS Act*.

A Complaint About the Nature of Security Screening Interviews

The complaint raised five issues:

- that the complainant was in receipt of a telephone call from a Service employee not involved with or aware of the fact that the individual was the subject of a security screening review;
- the Service put questions to the complainant that were outside its mandate to provide security screening advice in aid of the immigration program;
- the report written by the CSIS officer demonstrated a lack of respect for the applicant;
- the two interviews conducted by the Service were overly long; and
- that the screening and recommendation process was subject to unwarranted delay.

Overall, the Committee found that the Service acted in a reasonable and prudent fashion in handling the case. The time CSIS took to process the matter was not inappropriate under the particular circumstances involved, though the Committee was not able to address issues of delay in agencies of Government other than CSIS. While the Review Committee believed the "stray" phone call from a Service employee to be unfortunate and inappropriate, we concluded that it was made in error. It is important to note that in this instance the Service forwarded a positive security screening recommendation to Citizenship and Immigration Canada.

A Complaint About the Nature of Information Collected and Transmitted to CIC

The second case was based on the complainant's challenge of the accuracy of the Service's reporting. Our review was made more difficult by the absence of official transcripts of the Service's interview or a signed declaration by the complainant. We determined nevertheless that the CSIS investigators were inadequately prepared for the first security screening interview they conducted with the complainant. They had not reviewed the Personal Information Form (PIF) completed by the individual. In our opinion, this knowledge would have resulted in an interview that was focused and conducted in a more professional manner.

In addition, we took issue with a CSIS report to CIC where the Service stated that the complainant's representative was allowed to attend a security screening interview. We found that the investigators considered that the representative's attitude would not lead to a productive interview, and so the representative was asked to leave.

It is evident to the Committee that CSIS failed to transmit all relevant information to CIC about the complainant. We recommended to the Service that it forward all information necessary for CIC to reach a conclusion about the complainant's application.

Notes

- 1 *Report of the Special Senate Committee on Security and Intelligence*, January 1999.
- 2 It was determined that the definition in section 2(b) of the *CSIS Act* which refers to “foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,” was sufficiently broad to include serious transnational criminal activity.
- 3 Also referred to as “issue-based” targeting, the generic authorization names no specific persons but instead gives the Service wide discretion to investigate a class of activities fitting a threat that is described.
- 4 “*People and Process in Transition*”, Report to the Solicitor General by the Independent Advisory Team on CSIS, October 1987, and *The Intelligence Assessments Branch: A SIRC Review of the Production Process*, September 1988.
- 5 “*People and Process in Transition*”, p. 20.
- 6 “*People and Process in Transition*”, p. 35.
- 7 1987-88 SIRC Annual Report, p. 40.
- 8 1987-88 SIRC Annual Report, p. 41.
- 9 EXIPC was created in 1987 to ensure that intelligence production was consistent with the overall requirements and priorities of the Government, as well as with the specific needs identified by clients. EXIPC has met only rarely in recent years.
- 10 “Declared” intelligence officers are those the host country has been informed about by the foreign nation’s government and whose tasks are ostensibly related to legal, official diplomatic, and liaison activities. “Undeclared” officers are those about whom the host country has not been notified and who occupy posts within the diplomatic mission not openly connected with intelligence gathering.
- 11 A retention period is a time limit imposed on the Service for retaining a file. A Bring Forward (BF) date is assigned to the file based on the prescribed retention period for the file category. Upon expiry of the retention period, the Service reviews the files, and decides whether they should be retained, archived or destroyed.

- 12 Changes to certain warrant conditions were commented on in SIRC's 1997- 98 Annual Report.
- 13 *CSIS 36-97*, Federal Court of Canada, 3 October 1997, McGillis J. SIRC commented on the McGillis Decision in its 1997-98 Annual Report.
- 14 During the period under review, a warrant pertaining to a particular target group expired. CSIS applied for and was granted an additional warrant by the Court on the same target. The Committee reviewed applications for and the implementation of both warrants.
- 15 A replacement warrant is required when the Service changes the targets, the places or the powers of the previous warrant.
- 16 These sections of the *CSIS Act* pertain to the Service attesting that the facts presented to the Court justify the belief, on reasonable grounds, that a warrant was required to enable the Service to investigate a threat to the security of Canada.
- 17 The "resort to" clause permits the Service to use the powers granted in a warrant against a target at a place not named in the warrant, which it believes the target has resorted to or will resort. The legality of this clause has been confirmed by the Supreme Court of Canada in *Thompson et al. v. The Queen*, [1990] 2 S.C.R. 111.
- 18 The Intelligence Assessment Committee is composed of senior officials from the departments and agencies of the Government of Canada most concerned with intelligence matters.
- 19 The Communications Security Establishment is an agency of the Department of National Defence. As described by the Auditor General in his 1996 report to Parliament, *The Canadian Intelligence Community*, the CSE "analyses and reports on foreign radio, radar and other electronic emissions...and provides this foreign intelligence to Canadian Government clients."
- 20 SIRC Annual Report 1997-98, An Operational Audit of CSIS Activities, p. 47.
- 21 Pursuant to section 15 of the *CSIS Act*, the Service may conduct investigations in order to provide security assessments to:
 - departments and agencies of the Federal and provincial governments (section 13 of the *Act*);
 - the government of a foreign state (section 13 of the *Act*); and,
 - the Minister of Citizenship and Immigration (section 14 of the *Act*).

- 22 The number of government security screening investigations for the year under review was 2,424. The majority of field investigations were carried out for the Department of National Defence (659), CSIS (415), Public Works and Government Services (316), Foreign Affairs & International Trade (305), and less than 200 for the Communications Security Establishment.
- 23 The Service carries out immigration security screening investigations, including any necessary interviews.
- 24 CSIS investigators assume the primary responsibility for security concerns, listing the names directly with foreign countries, and the application of the security profiles.
- 25 Both the EII and the Point of Entry Alert System are administered by the Immigration Assessment Unit in the Counter Terrorism Branch. EII is one of many data banks within the Field Operational Support System (FOSS) used by Immigration officers for information, identification, and processing purposes. EII holds information on all persons who have entered any part of the Immigration stream (either for admission purposes or for removal), and identifies the types of documents issued to the applicants and any action taken by CIC.
- 26 When the Service believes that it is not in a position to render a recommendation to CIC concerning a citizenship application, it must seek approval from the Solicitor General to continue investigating the case and “defer” providing the assessment.
- 27 We informed ten individuals that their immigration-related complaints had to first be submitted to the Director of CSIS. Twenty other individuals lodged complaints to the Committee after they had been submitted to the Director.
- 28 A group of fourteen complainants said that they were being asked to inform on their compatriots if they wanted their applications to be treated expeditiously.
- 29 This is usually determined using information from either the Department of Citizenship and Immigration Canada or CSIS (under Federal legislation governing Access to Information and Privacy) or from the nature of the screening interviews conducted by the Service. If the delay is within the Department of Citizenship and Immigration Canada then SIRC does not have jurisdiction.
- 30 Within such period of time as the Committee considers reasonable (thirty days is the most usual).

- 31 Concerning a case first heard by our former Chair, the Committee ruled that the subject of the complaint was of such character as to fall within the class of persons described within paragraph 19(1)(g) of the *Immigration Act*: “persons who there are reasonable grounds to believe...are members of...an organization that is likely to engage in...acts of violence” that would or might endanger the lives or safety of persons in Canada, and thus are not admissible to Canada.

The Committee’s decision was appealed, with the Federal Court of Canada ruling that portions of 19(1)(g) contravened the freedom of association assured by paragraph 2(d) of the *Charter of Rights and Freedoms* in a manner that was not demonstrably justified in a free and democratic society. The Court referred the matter back to the Committee for reconsideration.

Another Committee Member (no longer with the Committee) was subsequently asked to rule on whether the subject of the complaint, a permanent resident of Canada, was a person described in paragraphs 19(1)(e), and 27(1)(c) of the *Immigration Act* as they existed on 29 May 1992, and that portion of paragraph 19(1)(g) of the *Immigration Act* that remained in force following the Federal Court judgement.

Having found that the subject of the Ministerial Report was a person described in paragraphs 19(1)(e) and 19(1)(g), the Member concluded that a security certificate should be issued. This latest decision is being appealed.

- 32 Although we noted in our last Annual Report that CSIS saw no difference between threats to “Canadian interests” and threats to “the security of Canada”, we were uneasy in that the former could be interpreted as giving the Service a broader mandate than the latter term.
- 33 Asia Pacific Economic Cooperation Conference.
- 34 The CSIS video explains the Service’s role to law enforcement and other agencies.
- 35 It was not until 1 July 1998, however, that CSIS assumed the responsibility for the security screening of all Department of National Defence personnel.