SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1993-94

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
Collect calls are accepted, and the switchboard is open
from 7:30 a.m. to 6 p.m. Eastern Standard Time.

Cat. No. JS71-1/1994
ISBN 0-662-61343-0

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

Dear Mr. Gray:

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 1993-94, for your submission to Parliament.

Yours sincerely,

Jacques Courtois, P.C., Q.C.
Chairman

Edwin A. Goodman, P.C., O.C., Q.C.

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

Rosemary Brown, P.C.

George W. Vari, P.C., O.C., C.L.H.

Where law ends, tyranny begins.

William Pitt, Earl of Chatham
1708-1778

Table of Contents

The Security Intelligence Review Committee at a Glance

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

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

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

To the extent that national security permits, the Committee reports to Parliament through its Annual Report. This is available to the public. It constitutes an evaluation of CSIS operations that would otherwise not be allowed to come under public scrutiny because of national security considerations.

The Committee also has the power to investigate complaints relating to CSIS. First, it can investigate complaints by a person about, ``any act or thing'' done by CSIS. It is not necessary that the person complaining be personally affected by what CSIS did.

Second, the Committee can review certain denials or revocations of security clearances affecting federal government employees, or job applicants, or persons who seek to sell goods or services to the federal government under contract.

Third, in a related vein, it can also review adverse security findings that would affect a person's right to immigrate to Canada or obtain Canadian citizenship. If the Committee finds a complaint justified, it recommends a remedy.

1. Introduction

The SIRC Mandate

July 1994 marked the tenth anniversary of the promulgation of the *Canadian Security Intelligence Service Act* (the *Act*). It is now ten years since the formation of Canada's first civilian security intelligence service, the Canadian Security Intelligence Service (CSIS), and the regime intended to ensure its compliance with the law: the office of the Inspector General of CSIS, and the Security Intelligence Review Committee (SIRC).

Traditionally, such anniversaries are an appropriate time to assess past performance and to take a fresh look at any persistent problems.

In general, the *Act* has accomplished what it was designed to do. The Service is operating effectively, and it is performing within the law and Ministerial Direction.

The Service is now on the threshold of losing the experience it inherited from the RCMP.

CSIS management is confident that the transition will proceed smoothly, and will demonstrate the effectiveness of CSIS' internal training policies over the past ten years. Having observed the Service at close quarters during all of this time, we too are optimistic.

As we said in our two most recent reports, CSIS is now, on the whole, an effective security agency which operates scrupulously within the law. However, there are two areas of CSIS operations that still give rise to public concern, and that often stimulate critical media reviews of CSIS' activities.

The first area of concern is the entry into Canada, as immigrants or refugees, of persons who have committed crimes or who have abused the human rights of fellow citizens in their home countries. When such persons are allowed into Canada, Canadians lose faith in the system that is supposed to prevent such people from coming here as residents.

It is important at this juncture to point out that *CSIS is not responsible for screening-out criminals seeking to enter Canada illegally, nor those who may have abused human rights.*

The media often attribute failures of the screening system to CSIS. The responsibility in these areas falls to the RCMP, Foreign Affairs, and Immigration. CSIS is responsible only for screening out people who would be a threat to Canada's national security. Of course, CSIS passes any information it has to Immigration, but it is not part of CSIS' responsibilities, or its statutory mandate, to search for evidence of Human Rights abuses or criminal activity. Moreover, CSIS is a domestic security service and has only a handful of officers outside the country. The other departments responsible have much larger staffs overseas.

However, whatever the bureaucratic division of responsibilities between Federal departments may be, many Canadians see the system, on the whole, as being too porous. Even though the number

of immigrants is over 250,000 persons each year, and the number of criminals of all sorts who are allowed into Canada is probably less than one tenth of 1 percent of that total, Canadians obviously believe that the screening system should be improved.

We do not believe that an immediate solution is at hand, but there are actions that could be taken to enhance the system's effectiveness over the medium and long term. A substantial improvement in the data banks available instantaneously to computers at overseas posts would be a significant step in the right direction. Further, *we consider the present number of CSIS officers tasked with immigration screening abroad to be inadequate* and it would be highly desirable to find sufficient resources to double their very small numbers. The present overseas staff carry an unreasonably heavy burden in this regard. A combination of more up-to-date, readily available, data on undesirable persons, together with a small increase in personnel could significantly improve Canada's ability to screen out undesirable immigrants. *The efficiency of the system could be further improved if the personnel involved worked as a team rather than simply as the representatives of departments having separate and distinct responsibilities.*

The second area of concern is the provision by CSIS of advice regarding Security Clearances to other government departments. CSIS does not decide which personnel require security clearances, nor does it decide the level of security clearance needed. CSIS simply processes the tens of thousands of clearances requested by other departments of government. From our point of view, it is long past time that the number and level of security clearances required again be rigorously re-evaluated. We believe such an examination could reasonably be expected to recommend drastic reductions. This would save a considerable amount of scarce resources that are now, in our opinion, expended unnecessarily.

The report which follows reveals in considerable detail the basis for our conclusions about CSIS' performance of its duties and functions. There are several points of criticism, because there are areas in which we think the Service could do better. But, on the whole, we think the Service is in a good position to face the challenges of its second ten years.

This chapter summarizes our review of two CSIS investigations: (a) the proliferation threat, and (b) a continuing counter-intelligence threat.

The choice of these CSIS investigations for in-depth review this year reflects the changing nature of threats to Canada since the end of the Cold War. In particular, it illustrates the fact that the collapse of the Warsaw Pact and the Soviet Union, while eliminating many of the threats that have affected us for a generation, has given rise to new dangers which now require more attention than the lingering antipathies of the Cold War.

Terrorism, in all its forms, is now the principal danger to the security of this country and to the well-being of Canadians. The underlying causes of terrorism remain much the same, but the virulence of violent activities stemming from rising nationalism, religious fundamentalism, and long-standing ethnic grievances, has increased radically as the rigid constraints of the Cold War have evaporated.

In this new more unpredictable world, a world in which many people seem prepared to commit atrocities to achieve their political or emotional goals, the proliferation of weapons of mass destruction poses extraordinary dangers to peaceful people everywhere.

(a) The Proliferation Threat

In recent years, the consensus amongst western democracies about what constitutes national security has been changing. The conventional elements — territorial integrity, internal stability, maintenance of one's position on the international scene — are now considered by many academicians and governments to be inadequate to the definition.

An expanded concept of national security can encompass a range of state and societal interests. Many western states, including Canada, have added the elusive concept of ``Economic Security'' and the better-defined ``Proliferation of Weapons of Mass Destruction (WMD)'' to their broadened definition of national security.

Historically, the Canadian Security Intelligence Service and the former RCMP Security Service have not considered threats to economic interests or proliferation activities to be priorities. In 1991, however, CSIS decided to scrutinize both sectors with more vigour through its Requirements-Technology Transfer (RTT) unit. Last year's SIRC Annual Report reviewed CSIS' investigations of economic security [1]. For 1993-94, we examined CSIS' counter-proliferation activities, the other half of the RTT mandate.

[1]. SIRC Annual Report 92-93. “Protecting Science, Technology and Economic Interests.” page 9.

We examined CSIS' investigations and analyses directed against the proliferation of destabilizing technologies. The general objectives of the review were to:

determine whether the activities under investigation constitute a threat to the security of Canada;

determine if CSIS' activities conform to the letter and spirit of legislation, ministerial direction, and the Service's policies and procedures; and

assess the extent to which personal privacy and individual rights have been respected.

To conduct this assessment, we reviewed CSIS' operational files and intelligence reports, and we met with Service personnel. The review also looked at public information, and one of our researchers attended two international conferences on the subject.[1]

The Program

CSIS' counter-proliferation program falls under the responsibility of its Requirements-Technology Transfer (RTT) Unit. The Unit is responsible for investigating and, in so doing, preventing the ``...proliferation of destabilizing technologies," which are defined as technologies that contribute to the development of weapons of mass destruction, their delivery systems, and advanced conventional weapons. The program began with little information or guidelines on how to begin to identify or investigate potential threats to Canada posed by these types of activities.

Although previously an autonomous unit within CSIS, during the past year the Unit was integrated into the Counter-Intelligence (CI) Branch. RTT Headquarters is the major centre for liaison and analysis activities with respect to counter-proliferation work. There are also RTT staff in the regions.

The range of RTT activities in the counter-proliferation area has been quite broad. Among them are: ``awareness/liaison briefings" to government institutions and relevant private sector corporations; the compilation of a database; and extensive liaison with a number of federal departments and foreign agencies.

The Investigations

CSIS conducts its investigations under *section 12* and *paragraphs 2(a)* and *(b)* of the *CSIS Act*. Starting in 1991, RTT received an overall authorization to identify individuals, groups, organizations or corporations involved in acquiring or transferring, from or through Canada or

[1] American Association for the Advancement of Science; Seventh and Eighth Annual Colloquia on Science and Security: ``*The Proliferation of Advanced Weaponry"* and ``*Trends and Implications for Arms Control, Proliferation, and International Security in the Changing Global Environment."*

Canadian interests abroad, technology that could be used to develop or expand foreign nuclear, biological or chemical warfare capabilities. The intent was that, with this broad investigative authority, the Service could identify where the threat lay and then concentrate on the persons and groups of concern.

RTT bases its investigations on the premise that Canada has been a source of supply, a diversion point, and a training ground for foreign powers seeking to acquire technology and expertise that could be used to develop or expand weapons of mass destruction.

CSIS and its allies estimate that no fewer than nine countries in Asia and the Middle East pose a proliferation concern to the West, some by acting as supplier nations to those seeking proliferation related technologies.

Corporations, middlemen, visiting foreign scientists, and technicians, as well as a small number of foreign students studying in Canada, represent a proliferation threat.

We concluded that, in 1991, CSIS had reasonable grounds to suspect a threat to national security arising from the proliferation of weapons of mass destruction. A broad-based authorization at the beginning of this investigation was seen by us as necessary for RTT to acquire knowledge of the issue.

The case for the renewal, in 1992, of the same wide-ranging authorization was valid, we felt, but it was based on some cases which were ambiguous with respect to the threat to Canada. We noted that:

> allegations that a foreign national allegedly stole important technical data were not confirmed and the material at issue was of disputed value;
>
> we saw no information to confirm that a foreign government monitors its nationals abroad, nor did we see evidence that the latter were coerced to participate in a proliferation programme; and
>
> the Service affirmed that a Canadian company illegally exported technology from one foreign state to another. A police investigation concluded that the export was legal. The Service asserts that a clandestine procurement operation was involved.

The file review also revealed that between 1991 and 1993, RTT investigated over 200 incidents/persons/organizations. Despite the assurances given by a member of the Service's executive to the Targeting Approval and Review Committee (TARC) that individual levels of investigation would be sought once the Service had identified persons engaged in proliferation activities, to a large extent this assurance was not respected. We questioned the heavy reliance

by RTT in 1992, and afterwards, on an issue-based authorization, although the Service affirmed that the broad scope was absolutely necessary in view of the emerging nature of the threat, the available resources, and the high level of accountability for RTT's activities.

Findings

In 1992 the Federal Government discontinued an inter-departmental group which supervised the exchange of visits and information between Canadian government institutions and certain communist states. With the demise of the group, CSIS and other former members wanted to establish a mechanism for identifying those individuals from countries of possible proliferation concern who may have been seeking to enter Canada for the purpose of abusing their access to Canadian facilities for weapons development purposes.

In conjunction with other government partners, the Service introduced a program to screen persons coming to Canada to study in scientific fields.

We asked about the legal basis of the program. First, we learned that it operates under *section 12* of the *CSIS Act* and not *section 14*, which defines the screening functions in the Service. Furthermore, the *Immigration Act* governs the admission of foreign visitors to Canada. The Service pointed out that the purpose of the program was to conduct a *section 12* investigation, and information of value to other departments was a secondary benefit. The Service's own statements, however, tended to emphasize the screening nature of the program. We also questioned the *Privacy Act* implications therein. We believe that *section 14* is the logical section under which to conduct this program.

We concluded that the referrals to CSIS HQ (headquarters) from the SLO (security liaison officer) posts were quite variable in quality and usefulness. CSIS had not prevented entry of individuals to Canada, but it had, in some cases, provided adverse information to Immigration as a result of the program.

Exchanges of Information with Other Agencies

In practice, the RTT counter-proliferation program cannot operate without the co-operation of both domestic and foreign agencies. The vast majority of the correspondence we reviewed from Canadian agencies is very supportive of CSIS' counter-proliferation efforts, although co-operation varies from agency to agency. A key Canadian Government agency wondered, for example, ``...what the Service could offer that is not already obtained through the current network (especially from their U.S. connections)." The Canadian agency later made considerable use of the Service's expertise.

CSIS is not alone in its focus on proliferation as an area of investigation. Many other governments are similarly engaged.

CSIS provides advice to Government on the results of its investigations through several channels. Most advice is supplied through the reports produced by the Service's Requirements Analysis and Production Branch (RAP) and through the contributions of that Branch to the collective assessments of the Intelligence Secretariat of the Privy Council Office (PCO). Other Service advice to the PCO includes Threat Assessments (Counter-Terrorism [CT] Branch) and routine operational correspondence and meetings.

One report we looked at concerned the possible exploitation of an international organization by a country seeking to acquire Research and Development (R&D) information in Canada. An officer of an international group allegedly engaged in suspect behaviour but we thought, after reviewing the incident, that CSIS had overstated the case.

Case Examination

We reviewed in considerable depth a case where CSIS had provided advice to a federal agency about an employee. The information was generally accurate, although we did perceive there to be some problems. The employee was dismissed by the agency as a result, in part, of the advice provided.

We expressed our concern about the Service conducting an investigation and then providing the results to another agency in a manner similar to a security screening. The manner in which the agency dismissed the employee removed the complaint/external review protections normally available to employees who are the subject of bona fide security clearance investigations. However, *section 41* was still available and the employee was informed of this avenue for redress.

Conclusions

This SIRC review sought to provide a comprehensive overview of RTT's counter-proliferation activities. It is our firm belief that the proliferation of weapons of mass destruction constitutes a serious threat to Canada's national security. There is a role for CSIS in this area, although perhaps not as prominent a role as one would expect to see in the case of counter-terrorism or even traditional areas of counter-intelligence. That said, we note that the Service has increased its credibility in the West's battle to contain the proliferation of weapons of mass destruction. CSIS has constructed a program from almost nothing and turned it into a valued service which is sought-out by other government agencies, both in Canada and abroad.

Based on our findings, we believe several key elements of the counter-proliferation program should be re-examined by CSIS.

Our conclusions and recommendations are that:

RTT relies heavily on an issue-based targeting authorization to conduct its investigative activities and says it is not able, in most cases, to seek more specific authorizations due to the new nature of the threat. We wonder whether the process should be streamlined, since the requirements may be too onerous given the ongoing nature of some of these investigations;

we believe that policy should be further elaborated to include the rationale (i.e. to acquire a working knowledge in a new field) and the objective (to focus the investigative effort) for these investigations. We are not, however, advocating the termination of the current issue-based authority. We do recommend that RTT management regularly review the investigations in order to consolidate those that should be submitted directly to the Targeting Approval and Review Committee;

RTT conducts a program under the issue-based authorization pursuant to *section 12* of the *CSIS Act*. We believe that the program should fall under *section 14* of the *Act*; and

some of the data held by RTT's counter-proliferation section deal with incidents which, in our view, are criminal intelligence. We question whether RTT, or even CSIS, should collect this information.

(b) An Ongoing Counter-Intelligence (CI) Investigation

In this review, we undertook to examine, as a whole, significant investigative activities undertaken by CSIS against a longstanding target of investigation. As we have done in earlier studies, we examined what CSIS was telling Government, what it knew, and the investigations CSIS undertakes; we looked at the full spectrum of CSIS activities in this area.

From CSIS Reports, we identified three threats to national security: classical espionage, theft of Scientific and Technical Information [S&T] (economic security), and foreign influence.

In terms of classical espionage, we noted significant cases internationally, some recent, involving the foreign power. In Canada, according to CSIS Reports, there is little recent evidence of actual activity. However, the lack of activity by diplomatic staff, according to CSIS, masks a range of long-term, low-risk activities best seen as part of ``an orchestrated whole."

CSIS considers threats pertaining to scientific and technological information, and economic security, to be the most damaging to Canadian security, due to the numerous levels in which it is carried out under the direction of a foreign government. According to the Reports, foreign nationals of that country are expected to collect information, and a significant number are directed to go further. Much of the activity is outside of the actual diplomatic (embassy or consulate)

structure. CSIS reports that theft of Science and Technology (S&T) and other information, ``...may be highly detrimental to the Canadian economy, especially to the export plans of companies which have invested in high technology R&D."

Intelligence activities, according to CSIS, also pose a ``foreign influence" threat. The foreign power's interference and attempted influence activities in Canada are wide-ranging and persistent, but seemingly innocuous. Most of them are legal. Such activity involves community manipulation, attempted control over their own foreign nationals and some endeavours, through the community, to lobby the federal government. A CSIS Report notes that the constant pressure to which the ethnic community may be subjected is a source of frustration to the community itself and, of course, impinges upon the freedoms guaranteed all Canadians in the *Canadian Charter of Rights and Freedoms*.

As part of our review, we examined factual accuracy against a wider reading of general files. In general, we found no factual errors, and we noted that the CSIS Reports make extensive use of open-source information and statistical data. In a few cases, however, we felt that information was slanted to make a point. Examples were given to indicate an intelligence activity. These examples, however, lacked crucial facts that might change how the events could be interpreted.

We were also concerned with CSIS' use of assumptions. By assumptions, we mean the use of statements prefaced by such wording as, ``It is probably safe to assume..." and the general use of the word ``probably." In our view, little in this business is as it seems, and all facts should be subject to rigorous scrutiny.

We also looked at measurements about the extent of the threat and damage.

In terms of the classical espionage threat, we noted that the target appeared to have a comparatively small number of intelligence officers in Canada. We had no useful estimate, however, as to the extent of non-diplomatic support. Another indicator suggested a low level of classical espionage activity. There appears to be little immediate threat, although much current low-level activity might be in preparation for future operations.

The threats concerning economic security and foreign influence are, admittedly, difficult to measure. In terms of foreign influence, we noted an apparent lack of complaints from the ethnic community; a fact attributed by CSIS to ``cultural conditioning." Theft of scientific and technological information rarely involves a tangible commodity, and potential damage is difficult to measure. To the best of our knowledge there is, as yet, no data base capable of comparing the threat posed in the S&T area, either: (a) over time (Has the threat increased or decreased over the last few years?) or, (b) by national comparisons (Do this nation's intelligence activities represent more of an S&T threat than those of other nations?).

We were able to examine other international assessments, which indicated the following:

inter-governmental consultation and threat assessment studies have been undertaken to determine whether S&T and foreign influence threats merit investigation;

S&T threats and foreign influence threats are sometimes assessed as being somewhat nebulous, and often unproductive to investigate;

some nations are considering a greater emphasis on protective security briefings to deal with possible S&T theft;

some nations are using public awareness campaigns to obtain assistance from ethnic communities; and

some nations appear to be scaling down their efforts against the intelligence activities in question.

We examined statistics on the resources dedicated by CSIS to investigation of the target. We also examined the case made for investigations, and the subsequent investigations based on the authorities provided.

Many CSIS investigations are conducted based on authorities against specific individuals. In our audit of randomly chosen individual cases, we had no difficulty with the authorization to investigate, or the subsequent investigations. In a few cases, we noted the lack of substantive facts as confirmation of intelligence activities. In one case, however, we noted that a businessman had offered a large sum of money for military and communications information.

Investigations are also conducted under a general authorization. The authorization is to, ``...determine the nature and extent of intelligence activity and assess the threat of such activity to the security of Canada." However, if CSIS officers come upon individuals who are potential ``threats," they must seek an authorization specifically against the individual to pursue investigations against him or her.

We examined the general authorization which is, in part, directed against the activities of a foreign intelligence service and, in part, against ``intelligence activities" undertaken by persons other than intelligence officers, sometimes but not always under the direction of the foreign intelligence service or foreign government agencies.

Our general review of investigations uncovered some problems, as evidenced by the fact that:

in a few cases, officers conducted investigations of the activities of individuals under the general authority, and without obtaining individual targeting authorization;

one investigation was of excessive duration;

in some cases, officers cited *paragraph 2(b)* of the *Act*, but did not make a case for ``clandestine" or ``deceptive." Also, authorities did not always fully address potential ``damage;"

underlying some analyses is a belief in the existence of a pervasive intelligence capacity, a belief challenged by some sources.

The nation in question does station intelligence officers in Canada and it does have a history of intelligence activities. The threat posed is, or could be, serious. We have no reason to believe that the resources directed by CSIS against the threat are excessive.

By all accounts, the threats posed by the intelligence gathering activities of this power are, at this time, nebulous, and sometimes hard to define. CSIS officers do an excellent job of providing Government with hard information on this subject.

The threats, while they may appear nebulous, are very real and so it is important that a convincing case be made that the tests in the definition of threat be addressed fully, and that potential damage be carefully assessed.

We have some reservations about the extent of the threat posed by non-professional intelligence collection, and are concerned that the net not be cast too widely.

We have recommended to the Director of CSIS that the investigations concerning economic security and foreign influence threats be reassessed, and that Government be consulted as to acceptable threat thresholds.

3. Case Studies

(a) Community Interviews

CSIS receives a relatively constant stream of information concerning the dangers posed by potential threats to Canada in ethnic communities. Unusual events in Canada, major upheavals, or a violent attack in another country, can prompt the Service to launch an investigation to seek more information about emerging threats at home.

In October 1990, as the Persian Gulf Crisis was escalating, the Canadian Security Intelligence Service initiated an interview program in Arab-Canadian communities. They conducted approximately 200 interviews. The Canadian Arab Federation and the British Columbia Civil Liberties Association, in particular, expressed concerns about the program. In its 1991-92 Annual Report, the Review Committee reported extensively on this first attempt at such a program.

Since the 1990 program, the Service has used community interviews frequently. In 1993, the former Director reported to the Minister that CSIS conducted interviews in several ethnic communities in Canada and added,

> ``The communities in which the programs were conducted were sensitized to the Service's role and mandate, which led to beneficial ongoing contact..." and,
>
> ``The programs allowed the Service to analyze and assess the potential for violence and to advise Government as appropriate .... To date, the Service has not had a single complaint concerning the most recent interviews, indicating that the guidelines and framework the Service developed for such interviews are working well."[2]

The purpose of our review was to verify whether CSIS indeed conducted the interviews in a proper manner. We raised the following questions:

> Were the programs duly authorized?
>
> Did CSIS collect and retain the information on a ``strictly necessary" basis in order to advise the Government about threats to national security? Specifically, did it collect personal information on those subjects interviewed?

Because interviews are an investigative tool, they are subject to Operational Policies and Instructions. The references in the CSIS Operational Manual state only the level of authorization necessary to conduct an interview (Level 2), and prescribe the principles and standards by which all investigations are conducted.

---

[2] Canadian Security Intelligence Service, *Annual Report 1992-93*.

One of the challenges of this review was to clarify the CSIS definitions of ``community interviews" and ``community interview program." Service policy says the following about community interviews,

> ``When interviews are conducted with leaders of communities and/or interest groups concerning threats to the security of Canada that may affect their community, employees must emphasize that the threat is being investigated and **not** the community itself."

In January, 1993 the Director General, Counter-Terrorism Branch issued, at the request of the former Director, a document which established the long-term objectives of the program, the rules for conducting interviews, and the guidelines for the investigators.

Taken together, the operational policies and the directives prepared by the Director General Counter-Terrorism Branch provide CSIS investigators with an in-depth framework to conduct community interviews. They contain most of the elements to maximize the information collected, with minimum damage to civil liberties.

However, we believe that, at the time of our examination, there were two crucial components absent from the policy framework. The first one is based on the fact that CSIS uses community interviews to gauge the potential for violence and foreign interference in a given community. The Service is merely asking community leaders for assistance in pointing to real or emerging threats.

It must not be forgotten that some émigré communities have lived through disagreeable experiences with security services in their homelands. In most of these communities, a knock on the door from the local security service can impact massively and adversely on the individual. Some may feel obligated to co-operate with CSIS. Consequently, we believe that *it should be mandatory that interviewees be told that interviews are voluntary.*

The second factor concerns CSIS policies and directives which stipulate that interviewees not be the subject of the investigation; they are merely asked to provide assistance to the Service. Consequently, we believe that, in Community interviews, investigative techniques should not be used to gather personal information on interviewees without proper Targeting Approval and Review Committee (TARC) authority.

In the first of the many community programs initiated by the Counter-Terrorism Branch that we reviewed, the interview reports did not raise any concerns. The investigators met with influential members of the community and the action plan developed by CSIS HQ provided the investigators with the tools to collect the necessary information.

Two targeting authorizations did concern us. One authorization did not cite the facts on which the investigation was based. This is contrary to a Ministerial Direction, which states that all

investigations must be based on facts and/or credible allegations and that CSIS must document them in writing. A second investigation was renewed despite the absence of the required justification. Notwithstanding these irregularities in the targeting approval process, we believe that the interview program was well planned and well executed.

A second community program we reviewed was considered by the Service to be the most successful. We agree that the program worked very well. It was a large one and covered different communities established across the country. Neither CSIS nor SIRC, has received a single complaint relating to interviews since those complaints received concerning the interview program related to the Gulf War. We also noted the great care that CSIS took in this program to not provide the authorities of one country with information on Canadian citizens whose origin was from another state which is in conflict with the first.

We questioned why, in a third community interview program, the investigator sought information about the interviewees from provincial authorities. This type of information is not, ``...strictly necessary to advise the Government about threats to national security." The program was otherwise well conducted by the Service.

The information the Service collected through its interviews in two more programs, and the advice it subsequently provided to Government, was consistent with the file information and was in compliance with its mandate. The Service has stated that the overall indications from its community sources were, ``...that the potential for violence here is low and, for the most part, the population in Canada supported United Nations' efforts to advance humanitarian aid."

An attack on an embassy prompted one interview program. CSIS conducted only two interviews. The interviews raised two concerns. First, community interviews require a Level 2 investigation: the interviews were conducted under a Level 1 authorization. Second, the interviews took place after the authorization had expired. We concluded that the Region did not adhere to the targeting policy.

Although the majority of the interviews in still another interview program were conducted without problems, we had some concerns. Even when an interviewer suspects that an interviewee is lying, that information is, nevertheless, often entered into the report. We rarely saw indications that the investigators recognized the traditional antipathy among members of persecuted communities towards the authorities. Adverse comments remain on the files without qualification. We advised the Service that we believe that *if a statement is at all questionable, it should be flagged and noted to that effect.* Of equal seriousness, we consider *CSIS did not respect the program guidelines when human sources were asked to comment on interview subjects.*

When we reviewed the interviews in communities undertaken by the Counter-Intelligence Branch, it appeared to us that there was some ambiguity as to what constitutes a community interview program. Most of the information we looked at represented isolated interviews with community

members, so that CSIS could learn about interference from foreign officials but little about the communities themselves. At least two other investigations had the same general objective, but focused on the events in the ethnic communities. In the latter cases, we think that special directives for such programs should apply.

In one investigation, an individual refused to be interviewed. The investigator insisted that the interviewee co-operate, and added that open information about CSIS could be provided. The individual accepted the information but refused the interview. We were uneasy about the manner in which the investigator sought the co-operation of the prospective interviewee.

Based on the information we reviewed in another investigation, we were impressed with a region's sensitivity to the factional politics operating in the ethnic community. The conduct of the Service's investigation protected both the reputation and the privacy of members of that community who, as it turns out, were unjustly accused.

Other investigations we reviewed raised questions about why a community celebration was reported on, why old Cold War information was still deemed relevant in a case, and why a person in contact with a foreign establishment was interviewed. We note, however, that these issues were isolated ones and we observed no problems with the vast majority of cases.

We concluded that, for the most part, CSIS learned and applied the lessons of its experience during the Gulf War. CSIS developed rules and guidelines which helped the investigators to carry out their responsibilities effectively. We believe, however, that these rules and guidelines omitted two crucial elements.

First, we think that interviewees should be told that interviews are voluntary. Second, we believe that investigative techniques should not be used to gather personal information on interviewees without the proper TARC authority. With respect to the first, CSIS adopted, in July 1994, a new policy which entirely satisfies our concern.

Our review also pin-pointed some difficulties in a small number of programs, but we found no systemic problems in how CSIS discharges its responsibilities. On the contrary, we were generally impressed with the restrained and appropriate manner in which the Service employees dealt with the leadership of communities which have been subject to abuse in their previous homelands.

(b) Sources in Government

In May, 1992, the Committee asked CSIS about the possible use of elected officials as sources. The Service, after a careful review, indicated to us that it was in compliance with the law and with

Ministerial Direction. We have subsequently found no information that would lead us to question that response.

This year, we examined operations that might touch upon federal, municipal, and provincial institutions. We found that there were few such operations and that many of them touched on federal, municipal or provincial institutions only in a most peripheral and indirect fashion.

We compared the policies covering federal departments and agencies with those dealing with provincial and municipal institutions, and determined that there were significant differences.

Federal operations are governed by a specific Ministerial Direction, released in 1986, and by a restatement of that Direction in the CSIS Operational Manual. Operations touching on municipal and provincial institutions are not governed by this body of policy.

When the Ministerial Direction was promulgated, the Minister instructed the Service and the Ministry Secretariat to develop policy governing operations touching on provincial and municipal organizations. Until 1993, nothing was produced. Following statements of concern in a report by the Inspector General, however, the Service and the Ministry of the Solicitor General agreed on the use of the ``Sensitive Institutions" policy to cover such operations.

The ``Sensitive Institutions" policy was first articulated by the then Minister in October, 1989. It provides for Service employees to seek approval, from senior CSIS managers, for operations that may impact on, ``...the most sensitive institutions in our society." According to the Minister, he provided the Direction so as to address his, ``...concerns with the effect of Service investigations on civil liberties."

CSIS has in place Memoranda of Understanding with every province. CSIS officers frequently call on the assistance of provincial and municipal officials. There is, in our view, a very good atmosphere of trust and co-operation at the present time. It is crucial that nothing taint these relationships.

In our opinion, the ``sensitive institutions" policy seems reasonable, so long as the basic principles of the Direction covering operations touching on federal institutions are extended, where appropriate, to provincial and municipal institutions.

(c) Potential for Political Violence in a Region

Each year we audit particular activities in one of the CSIS geographical regions. This year we examined the investigation of the potential for political violence in a specific region.

In early 1991, the then Solicitor General issued the Director of CSIS with the Cabinet's National Requirements for Security Intelligence. The annual instructions serve as a guide for the collection, analysis, and dissemination of intelligence pursuant to the *CSIS Act*. Last in the government's list of priorities was the issue of the potential for political violence.

We reviewed whether CSIS: had recently investigated the threat of political violence; had conducted investigations against individuals or organizations which were involved in, ``lawful advocacy, protest or dissent;" or had provided the Government of Canada with timely and accurate information concerning the issue.

We learned that since the Ministerial Direction was issued in April 1991, no investigations have taken place regarding the potential for political violence in that Region. This was also the year in which two ongoing investigations associated with violence in the region were terminated. Both were closely examined by SIRC before they ended. CSIS informed us that the Ministerial Direction authorized it to pursue such an investigation, should it become necessary. It was not deemed necessary during the several years preceding our inquiries.

One aspect of CSIS' primary mandate is to advise the Government of Canada about threats to national security. CSIS provides this advice through numerous publications and threat assessments. We examined all of the intelligence reports produced by CSIS to see if they dealt with the issue. Not one report focused directly on political violence in the region, although three did make very general comments about it.

We focused on one such assessment from 1991. This was a somewhat pessimistic analysis, which indicated that a sequence of events, if they transpired, could elicit political violence. We asked the Requirements Analysis and Production Branch (RAP) to provide the information on which it based its conclusions. We were told that RAP analysts used only open sources of information; they engaged in no inter-departmental discussions on the issue.

Our conclusions are that CSIS did not investigate the potential for political violence in the region and that, to the best of our knowledge, since the Service ended its inquiries in 1991, no person, group or organization has been so investigated.

We believe that the Service's analysis that the potential for violence is low, is generally correct. Some statements were tinged with pessimism, but the assessment accurately portrayed the situation.

Although a Ministerial Direction permitted CSIS to investigate the potential for violence in the region associated with an issue, the Service decided not to do so in the absence of reasonable grounds to suspect a threat to national security.

(d) Individuals Entering Canada

During the past fiscal year, we have been disturbed by reports that undesirable individuals who could represent threats to the security of Canada, had entered this country and bypassed existing controls. As CSIS plays an important part in screening individuals who apply to visit or immigrate to Canada, we examined the Service's role in three specific cases which had come to national attention. We point out, however, that in 1993 there were approximately 540,000 applications received to visit Canada and more than 200,000 requests to immigrate here. The vast majority of those visiting or immigrating pose no problems from a security standpoint.

(i) CSIS Role in Screening

Until July 16, 1990, all immigration applications received at Canada's missions abroad were submitted to CSIS' Security Liaison Officers (SLOs) for security screening and criminal trace checks.

In 1991, CSIS implemented its new screening program at all foreign posts. Under the new program, the key responsibility of the SLOs is to provide assistance and guidance to other departments only when requested to do so, and only on matters relating to immigration and visitor screening for national security concerns.

Since 1991, therefore, other Canadian Government officers conduct the initial assessment of applicants who wish to enter Canada. If the applicant meets the standard criteria for a security check, or if something of a suspicious nature arises, the case is passed to the SLO. CSIS screens immigrants to decide whether they fall under the *Immigration Act, paragraphs 19(1)(e), (f), (g)* and *(k)*.[3]

(ii) Three Cases

Two of the three cases we looked at pertain to individuals who are alleged to have been involved in crimes against humanity. In the first case, the individual was never referred to the Service. Hence, CSIS was not consulted on the security threat posed by the individual.

The second case involved a former senior government official of a regime which was infamous for its human rights abuses. He allegedly lied about his responsibilities in a war-torn state and was permitted to enter Canada. The SLO and Canadian mission staff from other departments failed to identify him. CSIS informed us that the country from which the immigrant came was submerged in chaos, and it was almost impossible to check the bona-fides of anyone associated

---

[3] *Paragraphs 19(1)(e), (f), (g)* and *(k)* of the *Immigration Act* stipulate classes of inadmissible persons, which include those where there are reasonable grounds to believe they will engage, or have engaged, in espionage, subversion, terrorism or violence likely to endanger the lives or safety of persons in Canada, and persons who were or are members of organizations which engaged in the same activities. This also covers ``retired'' terrorists.

with the government or, for that matter, originating from that country. The chaotic situation affected all western countries who were assessing refugee and immigration applicants.

The SLO interviewed the applicant; he lied about his government post and said he was fleeing the war. The SLO stated that there was no information in the immigration application form, nor was anything revealed in the interview that would have precluded his entry into Canada under *section 19* of the *Immigration Act*. Trace checks with other agencies, both Canadian and foreign, were conducted with no adverse traces reported.

In the conduct of this review, SIRC staff located public sources available to the en poste employees at the time of the interview which could have assisted in the identification of the applicant.

In the third case, another agency notified CSIS that it was searching for an individual it suspected of being involved in a kidnapping and terrorist bombing overseas. Prior to this notification, CSIS had no knowledge of the individual and there was little information available about the particular bombing incident. The Service checked and found that the individual had indeed entered Canada, but CSIS failed to locate him. The case was handed over to the RCMP who later learned that the subject had returned to his country of origin.

Our review established that the other agency notified CSIS about the suspect after his entry to Canada. The delay may have been due to that agency treating the case as a criminal rather than a security matter.

(iii) Conclusions

The objective of our review was to ascertain the nature of CSIS' role in allowing three individuals to enter Canada, and whether it had performed that role in an effective and efficient manner.

We learned that the Service's role was straightforward. In security cases, the SLO receives information from other agencies; he makes an assessment and provides feedback. In the first case there was no referral, and so there was no feedback.

In the second case, the refugee claimant was referred to CSIS. The SLO checked various documents and asked other agencies to do the same. As we point out earlier in this report, the SLO did not have the main responsibility for identifying this highly placed official of a government implicated in human rights abuses. We feel strongly that CSIS' overseas representatives should be given enhanced access to a more complete data base, so as to permit adequate identification in any future cases which arise. The Service has acknowledged that improvements can be made in terms of providing more support to its SLOs in this area.

The third case shows that CSIS was informed after the fact about the entry into Canada of a suspected terrorist. Subsequent to investigation, the case was handed to the RCMP, along with the information that the Service had collected.

The above cases indicate that CSIS actions, especially overseas where it has had a diminishing presence in recent years (see Foreign Arrangements, Chapter 4), are largely dependent on the actions and information provided by other agencies, both domestic and foreign.

We examined the cases which have come to the attention of the Committee since the formation of CSIS; we conclude that, irrespective of how effective the Service is in warning Canadian and foreign government agencies, problems in the communications systems of other agencies still have the capacity to neutralize the most vigilant and effective Service efforts. We urge that more be done to enhance the performance of CSIS' screening functions in ways that are fiscally responsible.

4. CSIS Operations

(a) Arrangements with other Departments and Governments

(i) Foreign Arrangements

As of March 31, 1994, CSIS had a total of 194 arrangements with 119 countries and 3 international organizations. The changes to arrangements in 1993-94 included three new arrangements with the security intelligence agencies in: former East Bloc countries which are no longer considered hostile; a temporary arrangement with a United States agency in view of potential terrorist violence; and a new arrangement with an agency in a stable African country. The human rights climate had dramatically improved in the last case and there was no information implicating that particular security organization in past abuses.

(ii) Domestic Arrangements

In 1993-94, the Committee reviewed only one domestic arrangement, an agreement between CSIS and the Atomic Energy Control Board. The agreement covers ``operational co-operation'' and the exchange of information between the two organizations. CSIS and the Atomic Energy Control Board may exchange information via threat assessments and other documents. They may also exchange information during meetings between the two organizations.

This agreement is similar to others with federal government departments. It is unique, however, in that it is the first formal *section 17* arrangement with a federal government regulatory agency. We have no difficulty with the agreement.

(b) Exchanges of Information with Foreign and Domestic Agencies

(i) Foreign Exchanges of Information

During 1993-94, the Committee reviewed samples of correspondence which CSIS released to foreign agencies via an overseas post. We undertook the study to ensure that there was no excessive or unnecessary use of powers by the Service. The SIRC review was conducted pursuant to *subparagraph 38(a)(iii)* of the *CSIS Act*, whereby the functions of the Review Committee are, ``...to review arrangements entered into by the Service pursuant to *subsections 13(2)* and *(3)* and *17(1)* and to monitor the provision of information and intelligence pursuant to those arrangements.''

When we audit CSIS' Security Liaison Officer posts and examine the information and intelligence exchanged with foreign agencies, we compare these activities to CSIS' policies and procedures, Ministerial Direction and, the ultimate authority, the *CSIS Act*. We also review new policies which were introduced during the past year.

CSIS published an important new policy on the disclosure of information and intelligence to foreign agencies. We reported on this policy last year, but the most critical element is that, ``The

flow of information and intelligence must be controlled to protect the rights of individuals and protect the security of the Service's operations." We looked at the information exchanges using these standards and the other policy requirements.

When this audit began, the Co-ordinator Field and Liaison and his staff provided administration and support services to the SLOs, monitored assessments of the foreign agencies, and co-ordinated the functions of the liaison advisers in the operational branches. In June 1994, this Unit was disbanded, the last remnant of the Foreign Liaison Branch. Its functions were to be added to the responsibilities of another section. We note that, in the span of a few years, the responsibilities of dealing with the requirements of the SLOs have devolved to an ever decreasing work-force and we are seriously concerned about CSIS HQ's capacity to meet the requirements of the existing overseas staff.

If CSIS acts on the recommendation in the Introduction to this report (see Chapter 1), additional staff abroad will require more, not less, co-ordination and support.

In past audits, we described the jumble of assorted telexes, which comprised the CSIS Foreign Liaison Guidelines, as outdated and sometimes confusing. We were pleased to note that, last year, CSIS produced a new ``Procedures Guidelines." The new manual addresses some issues of considerable concern to us. We have complained in several of our reports about the difficulty we have had in reconciling the records of SLO correspondence kept at the posts with those kept in Ottawa. The Guidelines show that up-dated instructions were issued in this regard. While this was a positive move, we continue to believe, and the Service confirmed, that the system is still awkward. For example, the post we audited this year had adapted the system of logging entries to make it work well for them. Unfortunately, the adaptation used only part of the standard form and thus was not in compliance with HQ's instruction.

In most of SIRC's previous audits, we complained that the human rights records of foreign agencies were not easily accessible to Headquarters analysts making decisions about what material should be denied or released overseas. The new, computerized reporting system addressed the problem by providing human rights information. SIRC will, of course, continue to consult external sources on human rights conditions concerning the posts we audit.

Another new computerized document assesses the previous year's activities at the post. This new product reflects what the operational branches deem necessary, such as the foreign arrangements in force, a history of the post, and the percentage of Canadian and foreign enquiries by operational sector. Last year, we considered the utility of much of the information in the new document to be problematic. The percentages of enquiries to the post were either meaningless (because the number of exchanges was not specified), or absent. In 1993-94, the problem was resolved. The required information is now provided.

In a major move, and one which we find surprising, CSIS management decided to close a foreign post which liaised with major allies. Another post in that region is expected to cover the liaison responsibilities; SIRC reviewed this second post last year and found it already had a considerable workload from several other posts which had closed in recent years. Adding the high volume of work from the newly closed post to the fully occupied one has the potential, we fear, to reduce the effectiveness of the liaison relationships with all agencies covered by the remaining post in the region. Indeed, in the just-released CSIS/Immigration evaluation of immigrant security screening (see Chapter 6), concerns were aired about non-resident SLOs who had to cover immigration programs in several countries.

We are concerned that this is *a problem area with potential for serious adverse consequences*, and we recommend that the Service review the manning of these liaison posts.

In addition to reviewing policy, SIRC reviewed a Security Liaison Officer (SLO) post which covers Asian countries. The SLO post liaises with the security intelligence agencies of four countries. The political situation in this region is characterized, for the most part, by violent secessionist movements. In this theatre, the often cruel and inhuman actions of extremists are all too frequently responded to by almost equally gross violations of human rights by the authorities. We reviewed the work of the Post against this background of internal conflict.

The SLOs are responsible for screening applicants for immigration status when Immigration believes there may be security concerns. We noted that no immigration applications were rejected by CSIS at this post in recent years. We were told that the persons of security interest, such as extremists, do not usually apply through normal immigration channels; they often choose to use other countries as their entry point into Canada.

SIRC conducted a review at the Security Liaison Officer post to ensure that the material sampled at HQ was representative of the information provided by the Service under foreign arrangements. The information exchanges were examined in terms of: the statutory basis for the retention, dissemination, or receipt of the information; conformity to the foreign arrangements; the accuracy of the information provided by CSIS and potential damage to the individual in contrast to the importance of the investigation; and the control provisions, including recording methods, for the information provided by CSIS.

One of the more frustrating aspects of liaison with the foreign agencies in the region is the length of time it takes to receive replies to CSIS inquiries. The duration can be days, months, or even years. The security and intelligence agencies and their police counterparts in the region are not computerized. Requests for trace checks are passed to local authorities, and their officials are

delegated to carry them out. This usually results in house-by-house field investigations which can span many months before the information makes its way back to the Service. The situation is unlikely to change in the near future.

Despite the sometimes abhorrent human rights records of countries in the region, the agencies with which CSIS does business are not those of concern to the major human rights organizations. Nevertheless, we are conscious of the fact that CSIS information may be passed to agencies so accused, especially in areas where major internal conflicts are present. The reality is that this is sometimes unavoidable.

We are extremely conscious of the possible consequences to individuals whom the Service draws to the attention of authorities in the region we audited. Adverse information about someone deemed to be an extremist can have absolutely devastating consequences to that person and his or her family. The accuracy of the information provided by CSIS must be a paramount consideration, as well as the importance of the investigation itself.

We were interested to note that the Service saw fit to provide information to agencies about persons who the Service did not see as engaged in terrorist activities, although these were fewer than those individuals considered to be security threats.

We concluded that the information CSIS provided to foreign agencies, through the post we audited, fell within the Service's mandate, was accurate, conformed to foreign arrangements in place, and reflected sound decision-making on the part of Service employees.

Consequently, we thought the CSIS employees here were performing most capably in a difficult environment; they were supported by the Service's operational branches at Headquarters which, in several cases we examined, probably contributed to the saving of lives of non-combatants. This, of course, is an important facet of the role of CSIS.

Earlier in this chapter, we noted our surprise with respect to the decision to close a post abroad, following closely upon the closure of several other posts in an increasingly important region. Looking at some of the recent studies and evaluations from SIRC and CSIS itself, as well as complaint cases, we believe that the foreign liaison program would benefit from more attention from the Service, not less, as seems to be the trend in terms of representation overseas.

(ii) Domestic Exchanges of Information

Under *subparagraph 38(a)(iii)* of the *CSIS Act*, the Committee is to review arrangements entered into by CSIS for the purposes of *subsections 13(2)* and *(3)* and *subsection 17(1)* of the *Act.*

These include: agreements covering security assessments;[4] exchanges of information; and general co-operation with federal and provincial government institutions, the RCMP, and other police forces. The Committee also is to, ``...monitor the provision of information and intelligence pursuant to these arrangements."

Each year, we review generally the state of co-operation between CSIS and other domestic organizations.

We also look for problems. To do so, we audit a large portion of all of the exchanges undertaken by CSIS in the course of the past year. Thus, on an annual basis, we examine about 6,000 actual exchanges; we sample certain high volume, low risk areas. We also visit two regional offices, of which there are six, to discuss any problems we have observed, and any problems they have identified.

In our audit, we assess whether exchanges comply with the *CSIS Act*, other statutes, and the agreements with other agencies. We examine whether intrusions to personal privacy are proportionate to the potential threat.

Our audits are based on a logging system instituted by CSIS. ``Logging" is a process which requires the placing of a code indicating who sent and who received the information. All exchanges can be tracked through the Service's computerized data base.

This year, we began with a review of the volume of exchanges. For various reasons, it is difficult to be precise. We estimate, however, that on an annual basis, CSIS was party to about 12,000 exchanges. Not surprisingly, we noted in some regions an increase in the volume of counter-terrorism related exchanges.

We also examined policy or other changes that might affect domestic exchanges, such as: new Memoranda of Understanding, new direction, and new legislation. A recent significant change to direction is the cancellation of the outdated policy on demonstrations and protests. We had previously recommended that CSIS replace this policy. We noted that CSIS also signed its first Memorandum of Understanding with a federal regulatory agency.

Further, we examined how well the logging system is working. The quality of our audit depends on the thoroughness of this system. On the whole, CSIS appears to have an effective logging system, although we noticed some inconsistencies. For example, information from oral exchanges and ``informal" visits was not always logged. In most cases, the omissions were described as ``human errors." In a few, however, they may have involved uncertainties as to what organizations are covered, and what constitutes an exchange. In particular, we raised the issue of whether, in some provinces, university employees fall under memoranda of understanding between CSIS and the provinces, and thus whether exchanges with them should be logged.

[4] There has yet to be any such agreement signed.

We also examined how well exchange agreements were functioning. We examined this both in the course of the audit and through specific questions to regional managers. Overall, we found no signs of problems, and information appears to be flowing smoothly between CSIS and the RCMP, and between CSIS and other police forces. Liaison Briefings, in which CSIS introduces itself to police forces and other government bodies, should improve the effectiveness of this aspect of CSIS operations.

We examined a number of specific issues in more depth.

We asked CSIS managers to review, and ourselves reviewed, any use of sensitive information, such as medical files or welfare records. We found only one such case of sensitive information; it concerned an instance where CSIS employees attending a training session sponsored by the Department of Employment and Immigration had asked that, where there might be risk of contagion, ``...the medical condition of a client be prominently noted on the file cover..." of the person involved.[5]

The matter was resolved by senior management in CSIS and CEIC, which agreed that such information would be communicated at the supervisor or managerial level, but that the Immigration Centre concerned would not indicate exact details, only whether a contagious condition existed.[6]

We also examined the use of information from other government departments. With but very few exceptions, we noted that CSIS was very diligent in its application of the *Privacy Act*. Previous inconsistencies in the definition of ``consistent use" appear to have been resolved.

Finally, we examined the passing of information concerning protests and demonstrations. CSIS noted that such information is passed to police forces when there is a likelihood of serious violence. We found no cases where the passing of such information infringed on legitimate protest and dissent.

In this year's audit, we concluded that the majority of exchanges we reviewed revealed no problems. The whole process seems to be maturing and running efficiently.

(c) Warrants and Warrant Statistics

Under the *CSIS Act*, Federal Court judges must authorize the use of certain powers, such as telephone intercepts.

[5] Letter from CEIC, 20 September 1993, on Vol. 3, 520-32.

[6] Memo dated 25 February 1992, on Vol. 3, 520-32.

Prior to the creation of CSIS, the Federal Government published annually the number of warrants approved for use. We have continued that practice:

Table 1
New and Renewed Warrants

	1991-92	1992-93	1993-94
New Warrants Granted	39	32	85
Warrants Renewed/Replaced	73	115	103
Total	112	147	188

We are told that the increase in the number of new warrants granted was mainly the result of administrative changes on existing warrants (which resulted in existing warrants being counted as new warrants). Numbers have also increased due to changing legal requirements. From our own data, we noted no significant increase in warrant-related activity.

These statistics must be interpreted prudently. One warrant can authorize a number of powers against a number of locations and individuals. The number of warrants, therefore, is not necessarily a good indication of the actual extent of the use of intrusive powers.

Under *section 28* of the *Act*, the Governor General in Council can make regulations concerning warrants and the hearing of warrant applications. No regulations were made in fiscal 1993-94, pursuant to *section 28* of the *CSIS Act*.

As part of our annual review, we asked CSIS about the impact of recommendations for changes arising from an April, 1992 internal review of the Warrant Process (see last year's Annual Report, p. 54). We learned that the streamlining has resulted in less time being required to process a warrant application. According to CSIS, the review has defined everyone's role within the process, eliminated the need for detailed regional submissions, and reduced bureaucracy.

We compile our own statistics concerning warrant affidavits. Our data cover various criteria, such as the number of persons listed in the warrant affidavit, the groups targeted, and the kinds of powers used. Each year, we send CSIS a number of questions based on these statistics.

In compiling our statistics, we take account of the status of individuals, that is: whether the targets are Canadian citizens, Landed Immigrants, or Foreign Nationals. Increasingly, CSIS does

not indicate the nationality of the individual in the affidavit; we tabulate these cases as ``unknown." We recognize that there is no legal requirement to enter the nationality of the target on the affidavit, but we think this information is pertinent.

According to our data, the number of Canadians or Landed Immigrants named in warrants remains in the same order of magnitude as last year; that is, hundreds not thousands. We will examine an apparently significant growth in the number of secondary targets listed in warrants to ascertain its significance.[7]

(d) Counter-Terrorism (CT) Branch

Both we and CSIS recognize that the Canadian public expects Government to attend to their personal and political security. The Service considers that serious political violence, whether foreign or domestic, represents the greatest threat to the security of Canada. This type of threat can escalate quickly and with immediate and serious results. To compound the problem, this type of threat can change rapidly into forms which require new and innovative responses from CSIS and other agencies of the Canadian Government. To cope successfully with the threat, the Counter-Terrorism Branch says it must develop and maintain a flexible forewarning capability in order to meet Canada's evolving security intelligence needs.

As part of its efforts to respond to and anticipate new developments in the changing face of terrorism, the Service has created a new unit; one of its early tasks will be to meet the challenges posed by Middle East terrorism. Last year, we reported on our review of Service investigations in this area.[8]

In another initiative to deal with ``The Shifting Threats" and public service renewal, the organizational structure of the Branch was streamlined to provide CT managers with more direct access to the Director General in charge of the Branch. Those functions which support the CT Branch investigations were also rationalized.

Threat Assessments

We report each year on the number of threat assessments produced by the CT Branch. It is through this type of document that CSIS rapidly alerts other parts of the Federal Government about present-day and emerging threats to national security which are of immediate concern. For

[7] By secondary target, we mean someone who is known to the Service, and whose interception may be required for investigative purposes. These persons are subject to inadvertent interception — they use the same phone as a target. See Vanweenan & Chesson vs. the Queen [1988].

[8] *SIRC Annual Report 1992-93*, Chapter 3, Middle-East Movements, page 20.

fiscal year 1993-94 the Threat Assessment Unit produced a total of 843 assessments. This represents a relatively insignificant decrease (not quite 5 percent) from the 1991-92 period, but 18 percent fewer reports compared with 1992-93.

When we asked what accounted for the major decrease, we were told that fiscal year 1992-93 was exceptional for threat assessment production. That year, for example, saw Canada host the United Nations Refugee Working Group, while the wars in the former Yugoslavia and elsewhere escalated. The year described in this Annual Report reflected a return to a normal volume of assessments.

Research Studies

In our last Annual Report, we commented on the functional analysis which the CT Branch prepared concerning community interview programs. We took that analysis during the year just past and compared it as one measure against both the CI and the CT branch investigations. We comment on the outcome in Chapter 3 of this Report under, ``Community Interviews."

We were unhappy to note that, due to resource constraints, this Unit did not produce any documents which could be described as a functional analysis. We see this development as a loss for the Canadian intelligence community as well as for the Service itself.

(e) Counter-Intelligence (CI) Branch

As part of the review, we question the Service about developments in the CI Branch.

We asked if there had been any significant changes in the CI Branch structure, organization, or size. The Branch indicated that they are experimenting with a different organizational structure. They also noted that the CI Branch continues to decline in size, and is now about 10 percent smaller than the Counter-Terrorism Branch.

We asked the Service if there had been any significant changes in the Branch's focus or philosophy of operations. The Branch noted that in the past there was little need to question the underlying reasons for most Counter-Intelligence investigations. Today's environment is more complex. In response, the Service is careful to establish strategic objectives behind each investigation, and frequently reviews investigations to ensure that they are well focused. Also, the Branch is increasingly consulting with clients — federal departments and agencies — in its overall planning and in carrying out Branch functions.

We asked how the Branch is dealing with the changing environment. CI noted that they have created a more flexible organizational structure, and are attempting to focus its investigative thrust on matters of importance to its mandate and to clients. It recognizes that many of its investigations would, ideally, be shorter in duration and that, in a climate of budget scarcity, it

will have to ``fine tune" the use of resources in investigations. The new environment will also require more seminars and conferences to keep officers abreast of changes, and will require new programs, such as Requirements — Technology Transfer (a program providing businesses with awareness briefings and the task of collecting information on technology theft).

In summary, the CI Branch recognises that, in the new environment, it has to improve client liaison and become more involved with other agencies and departments of government. It also has to bring a greater degree of co-ordination to the challenges being faced in the new environment.

(f) Requirements Analysis and Production Branch (RAP)

Last year, we observed that analysts from the Requirements Analysis and Production Branch who specialized in science and technology had been assigned to work in the Technology Transfer Unit. We were concerned about this development in the wake of our recommendations several years ago; decentralizing analysts to the operational units tended to hobble the development of RAP and lower its effectiveness in providing advice to Government.

The situation changed again in 1993-94. The Technology Transfer Unit, previously independent of the operational branches, was incorporated into the Counter-Intelligence Branch (see The Proliferation Threat, Chapter 2). This reorganisation resulted in the analysts' positions returning to RAP.

Aside from this development, RAP did not change markedly in structure. The Branch redirected strategic analysts to: countries associated with traditional CI threats, Economic Security, Proliferation, and Global Trends and Emerging Issues.

Commentary

In 1993-94, the Requirements Analysis and Production Branch published 12 issues of Commentary, the unclassified publication which deals with strategic issues. The studies cover the following topics:

1. The Rising Tide of Islamic Fundamentalism (I).
2. The Rising Tide of Islamic Fundamentalism (II).
3. Economic Espionage.
4. The Contemporary Armaments Trade.
5. Globalization and Japan's Information Needs.
6. Middle East Peace? (I)
7. Summary of Commentary Issues (#1-36).
8. Equity and National Security.

9. Crime and Migration in Eastern Europe.
10. Leadership in the Islamic Republic and the Hierarchy of Shi'a Islam.
11. Irish Nationalist Terrorism Outside Ireland: Out-of-Theatre Operations 1972-1993.
12. Russia — An Odyssey of Change.

Client Liaison

One of the Service's core mandates is to provide advice to Government. A primary means by which CSIS performs this function is through the publications issued by RAP. In past years, the driving forces behind the published analyses were mainly the requirements of CSIS itself and the results of annual surveys of client departments conducted by RAP. Two years ago, the emphasis placed by RAP on the requirements of the client changed significantly.

RAP now has a marketing and client liaison unit whose purpose is to determine the intelligence requirements of clients within the Federal Government, communicate these requirements to RAP personnel and, by the best means available, respond to them with assessments. To assist this effort, CSIS has developed a computer system to track who receives the RAP information and the level of satisfaction with the product. So successful has this been, that an overseas ally has adopted the same system.

We were informed by RAP that their readership includes some 400 clients in approximately 50 departments or agencies of the Federal Government. The unit also stated that they have distributed approximately 10,000 copies of their products to clients in the first three quarters of fiscal year 1993-94.

Another development, which recently came to our notice, was that RAP will issue special short bulletins, called ``Current Intelligence'' which will be sent to selected Deputy Ministers and other senior officials on topics relevant to their responsibilities.

We note favourably that the developments in the sector for client relations are quite impressive. From a review standpoint, the computerization of feedback from other federal departments represents another tool which we can access to assist our own analyses of the CSIS products.

Review of the RAP Product

The intelligence products which are produced by RAP are considerable in both the numbers of documents published in a year and the range of topics they cover. We can only effectively examine and critique the RAP publications in the context of those which relate to the areas we intensively review in a year.

This year, our major review emphasis was placed on Proliferation, and Counter-Intelligence. Almost all of the RAP reports we examined dealt effectively with the subjects. However, we did observe that some problems arose in the interpretation of events. On the Proliferation side, the Service exaggerated the significance of an incident which may have been a technical breach, but certainly was not of major concern. In a second case, a federal department took issue with the Service's position that there were proliferation concerns associated with two foreign states. The Service responded that an international group, not CSIS, originated the concern.

Referring to the study of the particular nation, in Chapter 2, under the heading ``The Proliferation Threat,'' we felt that the information was selectively used, in some cases, to highlight an intelligence concern.

(g) File Management

This section deals with the status of all CSIS file holdings, and any anomalies. We describe the total number of files destroyed, those sent to National Archives, and the number of new files created by category. Particular emphasis is placed on those files CSIS inherited from the RCMP Security Service.

In fiscal year 1993-94, CSIS reviewed a grand total of 100,567 files, destroyed 84,731 of them and sent 3,205 of historical value to the National Archives. The rest have been reclassified into other file categories.

We noted some major changes in the Service's file categories, almost all of which were decreases in numbers. There was an 80 percent decrease in the number of files retained on foreign nationals who were of interest to CSIS from a national security perspective. There was also a 38 percent decrease in the files on racist extremists, and a considerable drop in the number of files on their organizations. The number of files on organizations in Canada of counter-intelligence and counter-terrorism interest also dropped dramatically. The number of files concerning delegations or groups of Canadians travelling to countries of security concern similarly enjoyed a large decrease.

We should point out that decreases in the file count do not necessarily presage a reduced threat to Canadian security. They may instead represent changes in extremist group membership and affiliation, or the Service's concentration on the most dangerous elements in various movements.

The only exception to the decreases described above was in the files on persons of counter-terrorism interest who were not living in Canada. These increased by 63 percent.

Files Inherited from the RCMP Security Service

We have persisted in monitoring the fate of the approximately 510,000 files which CSIS inherited from the RCMP in 1984. We can now say that the end is in sight. During fiscal year 1993-94, the Service's special unit reviewed 71,965 files and retained 5,978 of them. The remainder were either sent to National Archives or were destroyed.

CSIS still has approximately 15,000 inherited files to review. For fiscal year 1994-95 the special review unit will process the remaining file categories and, in so doing, will complete the review and disposal program.

In summary, the disposition of these files for 1993-94 was as follows:

Total Reviewed:	71,965
Destroyed	63,260
Retained	5,978
National Archives	2,727

(h) Internal Security

In February, 1994, the FBI arrested Aldrich Ames, a veteran CIA officer and one-time head of the CIA's Soviet Counter-Intelligence Branch. Allegedly, he had worked for Soviet intelligence since 1985, had received $1.5 million in payments, and had continued to work in the CIA after failing routine polygraph tests.

The Committee has asked CSIS a number of questions in the Ames case. We want to know if any damage was done to Canadian security. We also want to know if the Service has or will reassess CSIS internal security measures. Because of the potentially extensive ramifications of the Ames case, we do not expect the assessment process to be completed for some time.

(i) Foreign Intelligence

``Foreign Intelligence" can be defined as information or intelligence relating to the capabilities, intentions or activities of a foreign state. Under *section 16* of the *Act*, CSIS can assist in the collection of such information within Canada. It cannot, however, retain the information for its own use unless it meets the requirements of *section 12* of the *Act*.

Each year, the Committee conducts a review of applications for *section 16* operations, and of information retained by CSIS from *section 16* operations. Under *section 16* of the *Act*, investigations cannot be directed at Canadian persons or corporations, and so we examine with care any information concerning Canadians that is retained by CSIS.

Each year, as part of our review, we also examine retention by CSIS of information from the Communications Security Establishment (CSE). As one of many consumers, CSIS receives reports from CSE. Some reports derive from *section 16* operations, some from other CSE operations, and some from information from allied intelligence agencies. Some reports involving national security, however, may go only to CSIS.

Generally, we would like to be able to examine all foreign intelligence retained by CSIS touching on Canadians. This year, however, we had difficulty doing so because of changes in how information was logged by CSIS, and because information was placed only on operational files. Within this limit, we found no indication that CSIS had retained excessive or unnecessary information from *section 16* operations or from CSE reports. Also, we found no indication of *section 16* investigations directed against Canadian persons or companies, and no indication of unwarranted CSIS use of CSE's investigative capacity.

One item we have noticed is that CSIS is beginning to cross-index CSE reports in the CSIS computer systems. In this way, CSIS can determine if there are relevant CSE reports when doing a search, and thus easily request the reports from CSE. We will be examining further this access in next year's audit.

(j) Statistics on Operational Activities

One of the roles of the Committee, under the *CSIS Act*, is to compile and analyze statistics on CSIS operational activities.

Over the years, we have built up a small but useful computerized data base. We use it frequently in our studies, as well as in our statistical reviews. As time goes by, we are increasingly able to use the database to see longer-term trends. We use statistics largely, however, as a basis for asking pertinent questions.

We keep a particularly close eye on person-year data, and certain other financial data. This helps us to identify areas where the Service is focusing its effort. To some extent, using this data, we can assess whether whole investigative efforts, as opposed to particular investigations, are in proportion to the threat.

Last year, we complained that CSIS had begun classifying data according to ``National Requirements" — broad classifications of threat such as ``foreign interference." The new system, in effect, obscured any connection to actual targets. As things transpired, the system proved unsatisfactory to CSIS and is now being replaced by something more akin to the pre-1993 system.

5. Complaints

(a) Scope

Quite distinct from our general review function, we conduct investigations in relation to complaints made by any person with respect to any act or thing done by the Service (*section 41* of the *CSIS Act*), complaints made by individuals who are denied a security clearance and are adversely affected in their employment with the Government of Canada (*section 42* of the *CSIS Act*), reports made to the Committee pursuant to the *Citizenship Act* or the *Immigration Act*, as well as matters referred to us pursuant to the *Canadian Human Rights Act.*

(b) Statistics

During the 1993-94 fiscal year, we received 30 new complaints, allocated as follows:

Complaints, April 1, 1993 to March 31, 1994

	New Complaints	Carried over from 1992-93	Closed 1993-94	Carried over to 1994-95
Security Clearances	4	2	5	1
Citizenship	0	0	0	0
Immigration	1	0	0	1
Human Rights	0	0	0	0
Section 41	25	3	26	2
Total	30	5	31	4

Of the 25 new complaints submitted under *section 41* of the *CSIS Act*, two remain unresolved. Seventeen involved persons who believed that they were being subject to illegal activities or undue surveillance by the Service. In such instances, we choose to comply with the policy of the Service, neither to confirm nor deny that a person is a target. Yet, we thoroughly investigated the allegations to ensure that:

the Service had not used and was not using its powers unreasonably or unnecessarily; and

the Service was performing its duties and functions effectively, efficiently and legally.

Four complaints related to the length of time required by the Service in conducting investigations in order to provide advice to the Department of Citizenship and Immigration. Two were resolved

in the midst of our involvement, and the complainants withdrew their complaints. We are still investigating the Service's activities in the other two instances.

The remaining four cases are among the Complaints, reported in Appendix C.

(c) Security Clearances

Under *section 42* of the *Act*, a complaint can be made to the Committee by:

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

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

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

The Government Security Policy (GSP) provides for two different types of personnel screening: the first deals with the assessment of a person's reliability and results in the granting or the denial of either a basic reliability status or an enhanced reliability status; the second deals with the assessment of a person's loyalty and reliability, and results in either the granting or the denial of a security clearance. Individuals who wish to challenge a negative decision based on the results of a reliability check may do so through current grievance procedures in accordance with *sections 91* and *92* of the *Public Service Staff Relations Act.*

Such a process is purely an internal matter. This year, we had to inform three individuals that we did not have jurisdiction to investigate the denial of reliability status, since in such instances a CSIS security assessment would not normally be required. The Service's security assessment is required only for security clearances and, therefore, only in such cases can we investigate complaints pursuant to *section 42* of the *CSIS Act.*

(d) Immigration, Citizenship, and Human Rights

For the year under review, we received one ministerial report under the *Immigration Act*, which will be reported on next year.

No complaints were received about refusals of citizenship nor were there any referrals from the Canadian Human Rights Commission.

(e) Historical Statistics

A review of statistics concerning Complaints in the 1992-93 SIRC Annual Report was misinterpreted. We believe, therefore, that it would be useful to present complete statistics covering the Committee's activities in this area since 1984.

Those statistics are shown here, and are based on the total number of letters of complaint, or complaint inquiries, under *sections 41* and *42* of the *CSIS Act*, received from the public, as well as appeals and complaints made under the *Immigration Act*, the *Citizenship Act*, and the *Canadian Human Rights Act*, to the end of 1993. While the majority of these complaints never reached a formal hearing stage, each one had to be assessed, and a file review or other more extensive action taken.

Table 1. Complaints Dealt With By Formal Hearings

a.	*Section 41 CSIS Act* (Complaints against the Service)	
	Total number heard	12
	Findings in favour of complainant	4
	Findings in favour of CSIS	8
	(In six of the eight cases found ``against'' the complainant, the Committee criticized CSIS on some aspect of its actions or policies.)	
b.	*Section 42 CSIS Act* (Security Clearance Denials)	
	Total number heard	38
	Findings in favour of complainant	27
	Findings in favour of respondent	11
c.	*Immigration Act* Cases	
	Total number heard	8
	Findings in favour of subject	1
	Findings in favour of exclusion or deportation	7
d.	*Citizenship Act* Cases	
	Total number heard	7
	Findings in favour of granting	4
	Findings for denial	3
e.	*Canadian Human Rights Act*	
	Total number heard	1
	Findings against complainant	1
	Total Hearings	**66**

Table 2. Section 41 Complaints Dealt With Administratively

a.	Complaints withdrawn or abandoned	28
b.	No SIRC jurisdiction to investigate (Includes 95 complaints not initially addressed to the Service)	175
c.	Complaints resolved satisfactorily without formal hearing	32
d.	Irrational or nuisance complaints	69
e.	Complaints unresolved at end of 1993	6
	Total of Section 41 Complaints Dealt With Administratively	**310**

Table 3. Section 42, Security Clearance, Citizenship, Immigration, and Canadian Human Rights Act Cases Dealt With Administratively

a.	Complaints withdrawn or abandoned	26
b.	No SIRC jurisdiction to investigate	22
c.	Complaints resolved satisfactorily without formal hearing (Includes 42 cases resolved by DND following SIRC intervention)	44
d.	CSIS withdrew objections in Citizenship and Immigration denials	5
e.	Complaints unresolved at end of 1993	1
	Total of Section 42 Cases Dealt With Administratively	**98**
	Grand Total of Complaints and Complaint Inquiries Dealt With Under All Categories	**474**

Analysis

An analysis of these statistics will show that fully one third of the complaints against CSIS which were heard in formal session resulted in findings in favour of the complainant. For the remainder, three quarters resulted in findings that included criticism of some aspect of CSIS actions or policies.

A significant portion of the Committee's work did not involve CSIS at all, but concerned complaints from individuals about the denial of a security clearance by the Department of National Defence. Over two thirds of those complaints heard by the Committee resulted in findings in favour of the complainant.

What is perhaps more important, is that the Committee's efforts in this regard resulted in the satisfactory resolution of 42 other complaints without the necessity of a formal hearing, and brought about a significant change in DND policies. This policy change had the salutary effect

of reducing the annual rate of security clearance denials in the Department of National Defence from hundreds to less than ten each year since then.

Over the years, the Committee and its staff have dealt with a large number of complaints administratively. Each of these required careful assessment and follow-up action of one sort or another. In many cases our investigation showed clearly that CSIS was not responsible for the action complained of.

The initiation of SIRC action, of itself, has resulted in the resolution of many complaints. In five cases, objections to permanent resident status, or the granting of citizenship, were withdrawn once SIRC became involved. In addition, many complaints were withdrawn by the complainants following an initial response by the Committee.

A significant number of complaints fell outside the jurisdiction of the Committee. In many cases, this was because the complainant had not given CSIS an opportunity to answer the complaint as required by the *CSIS Act*. In 95 such cases, the Committee heard nothing more after advising the complainant of the proper procedure.

6. Security Screening

(a) Security Screening

The Service's security screening activity falls under *sections 13, 14, and 15* of the *CSIS Act*, supplemented by Ministerial Direction and Service policy. It is the most visible and client-driven activity of the Service. The Service advises government departments on the following: government security screening, immigration and citizenship screening, refugee determination program, and screening on behalf of foreign agencies.

(b) Government Security Screening

The Service conducts investigations and provides security assessments to government institutions for employees of the public sector and for private sector contractors whose work requires access to information or assets classified in the national interest. Government institutions make the determination of the number of requests and the level requested pursuant to the Government Security Policy (GSP) promulgated by Treasury Board.

For the year under review, the Service processed a total of 42,673 government security clearance assessments which included: the Airport program, the Department of National Defence, the RCMP, and Foreign Checks. The processing time for government screening Levels 1, 2, and 3 on March 31, 1994, was 6, 20 and 98 days respectively.

Undeniably, the Government Security Policy has a major impact on the Service's Screening Program. Because of worldwide political changes, the Service has been conducting a review of the GSP with the Treasury Board Policy Centre. This review was deemed necessary to ensure that the GSP accurately reflected the changing threats being faced by the Government in protecting its assets.

Among the proposed changes to the Personal Screening Standards are the following:

> For the five-year updates of Level 3 (TOP SECRET) clearances, a full field investigation would no longer be routinely performed. It would only be conducted for cause, i.e. after a determination, based on available information, that a greater degree of screening was required; a credit bureau verification, a criminal record name check and an interview with the individual, by the Department, would replace the field investigation. For initial Level 3 requests, all indices checks, as well as a mandatory field investigation, would still be required;
>
> The current standard applied for Level 1 (Confidential) clearances, wherein a Criminal Record Name Check suffices, and fingerprints are only required ``for cause," would be extended to Level 2 (Secret) clearances. This should significantly expedite the processing of the bulk of clearances both on the contracting and departmental side; and
>
> Credit Bureau Checks would be optional for Level 1 and 2 clearances, with the responsibility for conducting the check resting with the originating department.

The Service should not feel an immediate impact because its personnel will assist other government institutions by providing the appropriate training for their new responsibilities. Over the long-term, however, the Service should realize both financial and personnel savings.

(c) Immigration Screening

As also mentioned in past Annual Reports, the Department of Employment and Immigration implemented a new Immigration Screening Program at all overseas posts in 1991. This program, designed to streamline the immigration screening process, involved the development of world-wide security profiles and focused on individuals of security interest.

As a follow up to the Immigration Streamlining Program, the Service and the Department of Citizenship and Immigration undertook a joint evaluation of the program. We consider the evaluation report to be well done, although we do not yet know what recommendations the two agencies will implement, nor when.

The report acknowledges that both the public and the Government expect that immigrants to Canada will have their background screened for security purposes. To do this in a cost-effective way requires balancing the security risk against undue delay in allowing legitimate immigrants into the country.

The evaluation provides a large list of findings and recommendations. Among them, the report acknowledges that the quality and effectiveness of immigrant security screening depends on the, ``...front-line officers making the decisions on (immigrant) admission to Canada." The evaluation calls for improved communication between CSIS and the Department of Immigration, including a better information sharing system in order to facilitate the detection of security risks. The report also calls for CSIS to train government employees abroad to be more security aware. We fully support improved training for officers involved in this vital work.

On average, the Service takes 31 calendar days to perform the security screening of an immigrant. Complex cases may require more thorough checks and more time. Hence, for a small proportion of cases, the screening may take between six months to two years. At the conclusion of its screening activities, the Service provides either a ``no objection" report or a detailed report, called a brief, as advice to the Department of Immigration.

From April 1, 1993 to March 31, 1994, the Service forwarded briefs on 62 individuals. Of the 62, two have been landed, landing is expected to proceed with two others, and one person was refused landed status. The other 57 cases are still outstanding.

(d) Citizenship Security Flag System

The Service provides the Department of Citizenship and Immigration with the names and biographical data of permanent residents about whom the Service has identified security concerns, thus justifying a closer look at the time of an application for citizenship. On March 31, 1993, the Citizenship Security Flag System contained the names of less than 100 Canadian residents.

(e) Refugee Determination Program

The Refugee Determination Program (RDP) processes the backlog of claimants who applied for refugee status prior to January 1, 1989. The two-year program, first scheduled to end December 31, 1990, was extended to March 31, 1993. Although the program was officially terminated at the end of March 1993, the Service continued to receive applications after that date for security processing under the program. The Service's timely and accurate advice is critical to Immigration Canada's refugee processing efforts. During the past year, approximately 900 new cases were received, of which 52 have yet to be finalized.

(f) Screening on Behalf of Foreign Agencies

Subsection 13(3) of the *CSIS Act* provides the authority for the Service to enter into reciprocal arrangements with allied services for the provision of security screening assessments.

These assessments are provided both on Canadians and on others who have resided in Canada. In each case, authorization is obtained from the individual in question before information is released to a foreign government or agency. In addition, cautions regarding the use of the information are placed on each forwarded document.

In fiscal year 1993-94, Security Screening processed 1,041 requests for foreign agencies, which required 170 field investigations. Of these investigations, only 2 resulted in detailed information briefs containing adverse information being provided to the requesting agency.

7. Regional Audits

(a) General

Each year, the Committee examines investigative activities in a single region of Canada. This review encompasses targeting decisions, warrants, investigations, surveillance, and sensitive operations. It is an update of how CSIS investigative procedures have changed over the last year, and a means of examining CSIS activities in a holistic, rather than single-faceted fashion.

The audit covers all Service activities in a region during a fiscal year. At the end of the year in question, we send out a draft work plan indicating how we propose to proceed, and we ask for comprehensive lists of targets, warrant affidavits, and other information. From these lists, we randomly select cases for audit.

Over the years, we have developed specific approaches and procedures for these audits. We try to obtain a picture of how much investigative activity is current, how many people are investigated, and whether warrant affidavits are in force in the particular region. We also examine new Service direction and instruction which governs the investigator's activities; this procedure is a pre-audit introduction to the cases which await us. We also examine whether CSIS activity is in line with direction and instruction, and the *CSIS Act;* lastly we conduct actual case audits.

There is a danger for auditors in following a set and predictable pattern. Consequently, for each audit, we try to go beyond the predictable; we examine a new aspect of regional operations. Last year, for example, we looked at CSIS instruction concerning investigative activities that might touch upon legitimate protest, dissent, and sensitive institutions. We also reviewed Ministerial Direction having to do with joint operations; that is, CSIS co-operation in Canada with allied intelligence services.

(b) Targeting

In November 1992, CSIS amended its targeting policy. The amendments include definitions of such terms as ``threats to the security of Canada," ``reasonable grounds to suspect," ``lawful advocacy, protest or dissent," and ``strictly necessary." The new policy also establishes a more precise regime for reviewing requests for targeting. Targeting policy now formally incorporates the following five principles:

1. All investigations must be in accordance with the law.
2. The investigative techniques used must be commensurate with the gravity and imminence of the threat.
3. The need to employ intrusive investigative techniques must be weighed against the possible infringement on constitutional rights and freedoms.

4. The more intrusive an investigative technique, the higher the level of approval required.
5. Except in emergencies, less intrusive techniques must be used before more intrusive techniques.

The adjustments to policy take into account the profound political changes in former communist countries, and provide instruction on techniques to identify emerging threats. The revised policies also focus on those persons who support terrorism or espionage in other states; for example, actions which would be considered a threat if directed against Canada. The next regional audit will take a closer look at how CSIS applies the latter policy.

We examined a number of cases and determined that all of the investigations were properly authorized. In the region concerned, we agreed that CSIS had reasonable grounds to suspect threats to national security, as the grounds cited were based on facts or credible allegations. The review revealed that an investigative technique in one case violated the expectation of confidentiality in a federally regulated sector. We concluded, however, that the investigative techniques used by the Service were commensurate with legal requirements and the nature of the threat.

(c) Warrants

Each year, the Committee examines a small number of warrant affidavits to ensure the accuracy of the information cited. This year we examined supporting documentation before the courts, and reviewed the warrant working files and warrant product (the information obtained from warrants).

In two large affidavits, we noted no serious concerns. Both seemed factually accurate and well-balanced. In one case, the Service had specifically addressed the changing world situation. We found a small number of minor problems. In another case, we noted that the information in the affidavit was more dated than the context might lead a reader to suspect. In yet another, we noted an instance of apparent ``circular reporting." In effect, the Service officer, in the affidavit, may have cited a source which had originally received the information from the Service itself. According to CSIS, ``The Service made an effort to get to the bottom of this question but was unable to verify one way or the other, and so the case was treated appropriately."

In our review of the application of warrant powers and warrant product, we look at how authorized powers are actually used, how individuals come to be listed in warrants, the treatment of any intercepted solicitor-client communication, and other matters. In this audit, we found no problems.

In a number of circumstances, we noted that the application of warrant powers changed, frequently due to Court rulings in Criminal Code cases. This matter is under active discussion with the Service in order to determine the extent to which decisions made by the Courts in criminal matters should be applicable in the national security context.

(d) Surveillance

Under new rules in the CSIS Operational Manual concerning targeting, promulgated in November 1992, the Service can undertake ``temporary'' emergency surveillance coverage, ``...in circumstances where an unanticipated national security threat is suspected.'' CSIS officers usually require a targeting authorization before conducting any investigative activity. We have no problem with the new provision, but we will, from time to time, examine its use.

We examined a number of cases where surveillance was used, and saw no problems. Again this year, we asked about the use of video cameras, and when a warrant is or is not required. We were told, subsequent to the R vs. Wong decision, that the Service must make a case-by-case judgement as to whether an individual might have a ``...reasonable expectation of privacy.''

(e) Sensitive Operations

We examined a number of operations approved by the Minister, and a number approved by senior CSIS managers.

Under Ministerial Direction, the Service is to retain control over any operation involving a foreign intelligence service on Canadian soil; this is a fundamental issue of sovereignty. In one case, a meeting took place without a CSIS officer being present.

Finally, we examined operations touching on sensitive institutions, the media, religious institutions, and legitimate dissent. Such operations must be approved by senior CSIS managers. We found that all such operations were appropriately managed, and were justified given the nature of the threat.

8. Review of General Matters

(a) Ministerial Direction

Under *subsection 6(2)* of the *CSIS Act* the Solicitor General may issue direction to the Service. The Committee not only reviews all new directions issued, in and of themselves, but also examines how well they work, and how well they are being followed.

In 1992-93, we received two new Ministerial Directions: ``National Requirements for Security Intelligence 1993-94," and a second concerning ``Sensitive Operations." In the ``National Requirements" public safety was, ``...reconfirmed as CSIS' top priority," and CSIS was directed, ``...to maintain flexible forewarning capability." The ``National Requirements" are composed of:

1. Counter-Terrorism
2. Counter-Intelligence
3. Security Screening
4. Economic Security
5. Proliferation
6. Assistance to Foreign Intelligence
7. Developing Relations with Former Adversaries

The National Requirements for 1993-94, it is worth noting, were not released by the Minister to the Service until July, 1993, some three months into the fiscal year.

The ``Sensitive Operation" direction involves the reporting and treatment of minor breaches of standards.

(b) The CSIS Operational Manual

We examine changes to CSIS internal guidelines, as found in the CSIS Operational Manual (OM), as if they were Ministerial Directions. Almost every study conducted by SIRC begins with a review of Ministerial Direction and the CSIS Operational Manual.

In 1993-94, we counted a total of 12 changes to the CSIS Operational Manual. The changes involve:

the implementation of *section 21* warrant powers;

the conduct of investigations. This direction, ``...provides the principles and standards for all investigations," and covers general policy areas such as, ``sensitive institutions" and legitimate protest and dissent. It articulates earlier Ministerial Direction, information handling respecting high profile persons, and the right to counsel when detained under the *Immigration Act.* This instruction indicates what CSIS investigators must tell detainees before undertaking interviews;

operational co-operation with foreign agencies. This instruction, in part, articulates existing *6(2)* direction;

operational use of the polygraph. This instruction, in particular, contains guidelines for obtaining consent; and,

operational contact with members of political institutions. All interviews with elected officials, except security screenings, must be authorized by senior managers.

In addition to the above, one instruction involves a licensing matter, and one involves internal security. Four other instructions concern minor wording or administrative changes.

According to CSIS, all policies predating the *CSIS Act* that were originally contained in the Service's Operational Manual have now been removed, and the majority have been replaced with new Service Policies. In previous years, the Committee has commented on the existence of outdated instructions.

On a number of occasions, we identified and pointed out to the Service discrepancies between the English and French versions of new CSIS Operational Manual policies. For example, in the CSIS policy describing operational procedures for Citizenship Screening, the English version states approval must first be granted by the Solicitor General before providing advice to the Departments of Citizenship and Immigration recommending the refusal of a citizenship application. In French, the reverse instruction is provided, requiring CSIS to obtain permission from the Citizenship and Immigration Department before recommending rejection to the Solicitor General.[9]

In the CSIS instruction, Conduct of Investigations, there is direction provided concerning CSIS employee contact with members of the judiciary. In the English version, contact includes all judges at the ``higher court level," while in the French version there is reference to contact with judges of the Supreme Court (Cour Suprême).

In the 1990-91 Annual Report, the Committee noted the ``patchwork" of instructions governing the use of warrant powers, adding that, ``...the Service needs comprehensive guidelines on the use of its most intrusive powers."[10] This year, CSIS indicated to us that, ``...a draft policy relating to the acquisition of warrants has been completed and is to be submitted shortly to the Director for his approval." The completion of this work will, apparently, finalise the Service's work of developing a comprehensive policy covering the acquisition and use of warrants, and the treatment of information derived from warrant operations.

[9] A correction was published by CSIS in January 1994.

[10] *SIRC Annual Report 1990-91*, page 4.

(c) Disclosures in the Public Interest

Section 19 of the *CSIS Act* prohibits dissemination of information obtained by CSIS in the course of its investigations, except in a number of specific circumstances. It does not, however, restrict the Solicitor General from disseminating information provided to him by CSIS.

Under *subparagraph 19(2)(d),* the Minister can permit CSIS to provide information to, ``...any Minister of the Crown or person in the public service of Canada..." when the public interest outweighs any invasion of privacy that could result. There were no disclosures under *subparagraph 19(2)(d)* in 1993-94.

According to the CSIS Operational Manual, the Service can recommend that the Minister release, or have CSIS release as the agent of the Minister, information obtained from operations. There were no such releases in 1993-94.

(d) Regulations

Under *subsection 8(4)* of the *CSIS Act*, the Governor General in Council may make regulations concerning the appointment and management of CSIS personnel. CSIS received no such regulations in 1993-94.

(e) Report of the Director and Certificate of the Inspector General

Section 38 of the *CSIS Act* lists the functions of the Security Intelligence Review Committee. The first specific function listed in the section is to, ``...review the reports of the Director and the certificates of the Inspector General."

The Report of the Director is usually submitted to the Solicitor General in July following the end of the fiscal year. The Director gives a copy to the Inspector General who is required by the *Act* to submit a certificate to the Solicitor General stating the extent to which he is satisfied with the report and commenting on CSIS's compliance during the year. We normally receive the Inspector General's Certificate in the Fall.

We usually receive the Director's report in late June; this year, we received it in late July, too late for inclusion in this year's review. We will report in depth on the 1993-94 report in next year's SIRC Annual Report.

We received the 1993 Certificate of the Inspector General in November 1993. In her comments, she noted that the 1992-93 annual report from the Director to the Minister provided a reasonably accurate, comprehensive, and balanced account of CSIS activities. She added, however, that the report was as silent as the previous year's about problems and their effects on CSIS operations,

and that it did not, on the whole, provide sufficient contextual information or analytic commentary to illuminate the dimensions of particular security threats. The Service addressed these concerns to the Minister's satisfaction.

In discussing compliance issues, the Inspector General noted that certain sensitive operations had not received the prior approval of the Solicitor General, required by Ministerial direction. She also commented on CSIS' approach to reporting suspected illegal activities to the Solicitor General under *subsection 20(2)* of the *Act*, and on the measures used by CSIS to protect its operational information.

(f) Reports of the Inspector General

Under the *Act*, we can ask CSIS or the Inspector General to, ``...conduct a review of specific activities on our behalf." We have, in the past, never asked CSIS to conduct such a review. We made no such request of the Inspector General in 1993-94.

The Committee is able to take advantage of the in-depth reports prepared by the Inspector General on behalf of the Solicitor General. In 1993-94, we received three such reports, one dealing with sensitive operations, on which we commented in our 1992-93 Annual Report. The other two reports examined the protection of information in CSIS operational files, and the state of CSIS and RCMP cooperation.

In June, 1993, the Inspector General, responding to a request from the Solicitor General, provided a case study concerning CSIS's measures to protect operational information. In her conclusion, she noted the extremely sensitive nature of CSIS information holdings and said that CSIS must appropriately protect them against improper access from both inside and outside the organization. She attributed problems revealed by the case study to gaps in policy and procedures, noting that when such gaps result in unclear rules, roles, and responsibilities they impede appropriate action and undermine accountability. She added that, ``...the Director recently introduced initiatives to address some of the problems that were identified."

A second report, in July 1993, reviewed CSIS activities under the 1989 Memorandum of Understanding between CSIS and the RCMP. The agreement governs operational cooperation between the two agencies, including exchanges of information and provision of support and assistance. In the report, the Inspector General concludes that the implementation of the Memorandum of Understanding, ``has resulted in a noticeable improvement in the exchange of information and intelligence between CSIS and the RCMP." However, she does recommend that the agreement be supplemented with procedures to ensure consistent CSIS-wide interpretation and application. She also sees the potential for sources of ``tension." For example, the overlap of CSIS and RCMP mandates in certain areas, and the need for the protection of sensitive CSIS information ``in light of jurisprudence developing from the *Canadian Charter of Rights and Freedoms*."

(g) Unlawful Conduct

Under *subsection 20(2)*, the Director reports to the Minister any instances where he believes an employee may have acted unlawfully in the purported performance of the Service's duties and functions. The Solicitor General, in turn, reports such incidents to the Attorney General and provides the Committee with a copy pursuant to *subsection 20(4)* of the *CSIS Act.*

In 1993-94, we received one report under *subsection 20(4)*. The Committee also received a complaint from the individual concerned. In this case the individual is believed to have passed information to unauthorized individuals, thus contravening *section 122* of the *Criminal Code* (criminal breach of trust), *paragraphs 4(1)(a)* and *(d)* of the *Official Secrets Act* and *section 126* of the *Criminal Code* (disobeying a statute).

During 1993-94, the Committee continued to investigate one case from the previous year.

In last year's Annual Report, we delayed commenting upon a particular case since, we considered, it was likely to be the subject of a formal complaint. It was not, and so we address it now.

In this case, the individual's activities may have constituted a breach of trust by a CSIS officer, contrary to *section 122* of the *Criminal Code*. There may have been unauthorized disclosures of CSIS information, pursuant to *section 19* of the *CSIS Act*, and a possible violation of *subsection 126(1)* of the *Criminal Code*, and *paragraphs 4(1)(a), (c)* and *(d)* of the *Official Secrets Act* (care and treatment of classified information).

(h) SIRC Consultations and Inquiries

(i) Formal Inquiries

In our review function, not counting inquiries arising out of complaints, we directed 158 formal inquiries to the Service in the 1993-94 fiscal year (April 1, 1993 to March 31, 1994). The average time CSIS took to answer a formal inquiry was 49 days.

(ii) Briefings

We met with the Director of CSIS on October 21, 1993 and again on April 13, 1994.

We visited regional offices of the Service when our regular meetings took us out of Ottawa. We were briefed on regional operations in Toronto on September 22, 1993, Montreal on November 16, 1993, and Vancouver on February 9, 1994.

(iii) Beyond CSIS

We met with the Solicitor General on August 10, 1993, and again on January 11, 1994.

(i) Special Reports

Under *section 54* of the *CSIS Act*, we can make special reports to the Solicitor General on any matter relating to the performance and functions of the Service. In 1992-93, we submitted the following study to the Minister under *section 54:*

1. Counter-Terrorism Study 93-04, December 1993 (SECRET) *

A list of earlier SIRC studies can be found in Appendix B of this report.

9. Inside CSIS

In this chapter, we turn to the internal affairs of the Service.

(a) Recruitment

Since 1984, with the exception of one major relapse in 1986, CSIS has attempted to steadily redress the overwhelming predominance of males in the vital Intelligence Officer category of employees. To achieve this, CSIS has maintained a policy of recruiting equal numbers of male and female applicants in its training program each year.

Recently, budget reductions have constrained the Service's ability to recruit new Intelligence Officers. With fewer new entrants each year, it seems inevitable that progress toward the goal of equality between the sexes will now be slower than the Service or we would wish.

During the 1993-94 fiscal year, CSIS conducted one Intelligence Officer Entry Training class. There were fourteen recruits, five of those were conversions from other job categories within the Service. Efforts to achieve an equitable distribution of the sexes have continued, and eight of the fourteen recruits in this class were women.

In last year's annual report, we said that there were 47 percent female employees in the first level Intelligence Officer (IO) category. What we did not point out, however, was that in the overall IO category there was a total of 20 percent female employees. The percentage has improved again this year with the total of female employees now being 24 percent.

There is little difference in the statistics for the senior management level categories. The percentage of men remains the same as last year at 89 percent, outnumbering the percentage of women at 11 percent.

The representation of designated groups in the senior management level category is as follows: one member of a visible minority group, and one aboriginal person.

The overall representation of designated groups is compiled through the Service's self-identification program. Currently, aboriginal peoples represent 0.95 percent of the CSIS population, members of visible minorities 3.1 percent, and persons with disabilities 2 percent.

(b) Public Relations

The Service has a Communications Branch which deals with external enquiries. While *section 19* of the *CSIS Act* prevents these employees from confirming or denying specific CSIS

operational activity, they are able to provide verbal and written unclassified information regarding the role and functions of the Service, and the environment in which it operates.

The Director General of RAP, for example, addressed two British Columbia chapters of the Royal United Services Institute, as well as the Michigan Branch of the English Speaking Union of the United States. The latter address is to be published in ``Canadian Speeches.'' An article, based on the Director's address to Queen's University, was published in the magazine of the Royal Canadian Military Institute, winning that publication's award for best contribution of the year. Another address by the Director on ``Economic Espionage'' was published in the Newsletter of the Federal Association of Security Officers; and the Service released its second Public Report.

In addition, the Minister tabled the third annual CSIS Public Report on April 11, 1994.

(c) Accommodations

The newly constructed National Headquarters building is proceeding on schedule. Phase I is completed and Phase II is forecast to be completed and occupied by April 1995.

(d) Finances

This year the Committee received three one page charts concerning CSIS expenditures. In effect, we received an, ``Overview of CSIS Expenditures and Funding'' (basically a reconciliation between the Estimates and Actual Expenditures), ``Expenditures by Standard Object'' (a breakdown of expenditures by standard categories), and ``Other Expenditures'' (basically a general breakdown of covert expenditures). With these charts, we also received very brief explanations of variances.

In the Spring, the Government released a three figure breakout of CSIS spending, based on the Main Estimates. Below are actual expenditure figures for the 1990-94 period:

Table 1.

ACTUAL EXPENDITURES
($,000's)

	Personnel	Other Expenditures[12]	Capital[11]	TOTAL
1990-91	118,000	61,355	25,545	204,900
1991-92	120,956	69,200	15,294	205,450
1992-93	124,926	72,591	27,833	225,350
1993-94	118,819	77,282	48,190	244,291
1994-95[13]	115,101	74,537	17,196	206,834

As part of our work, we examine the data provided by CSIS with prior year data in our computers and query CSIS about significant changes.

The spending jump in 1993-94 is due to an additional $20 million dollar expenditure for the new CSIS Headquarters building, as a result of cash reprofiling from future year's budgets to 1993-94. The sharp decline budgeted for 1994-95 reflects budget cuts ($8 million in 1994-95) and completion of the new Headquarters building.

[11] Represents construction costs for the new Headquarters building.

[12] Predominantly other operating expenditures.

[13] Budget, based on Main Estimates.

10. Inside SIRC

(a) Accounting to Parliament

On January 18, 1994, the Solicitor General tabled the Committee's 1992-93 Annual Report.

The Committee appeared before the Standing Committee on Justice and Legal Affairs on May 10, 1994, to answer questions about its 1993-94 Main Estimates.

(b) Staying in Touch

We met with: Mr. Peter Russell, Professor of Political Science at the University of Toronto on September 21, 1993; Jean-Paul Brodeur, Director of Le Centre International de Criminologie Comparée, Montréal, on November 15, 1993; and, Mr. Colin Gabelmann, Attorney General of B.C. on February 8, 1994.

We are also helping to support the Canadian Association for Security and Intelligence Studies (CASIS) conference on, ``Intelligence Analysis and Assessment'' to be held in Fredericton, New Brunswick from October 27-29, 1994.

(c) Spending

Our 1993-94 budget is set out in Table 2 at $1,460,000; it represents a decrease of 3.3 percent from the budgeted spending of $1,510,000 in 1992-93. Our 1994-95 Main Estimates of $1,409,000 represent a further decrease of 3.4 percent from the 1993-94 budget.

During the 1993-94 fiscal year, we returned a total of slightly more than $150,000 to the Government, reducing our budget by a further 10 percent.

Table 2. SIRC Budget 1993-94

	1993-94 ($,000's)	**1992-93 ($,000's)**
Personnel	803,000	828,000
Goods and Services	648,000	673,000
Total Operating Expenditures	1,451,000	1,501,000
Capital Expenditures	9,000	9,000
Total	**1,460,000**	**1,510,000**

Source: 1993-94 Estimates, Part III, Section II, Figure 7

(d) Personnel

The Committee has engaged a small staff of fourteen in total: an Executive Director; a Senior Complaints Officer to handle complaints and ministerial reports; a Director of Research Counter-Terrorism; a Director of Research Counter-Intelligence; and four Research Officers; an Executive Assistant who co-ordinates activities on behalf of the Chairman, conducts all media liaison, co-ordinates the production of the Annual Report, and undertakes research projects; an Administrative Officer who is also the Committee registrar for hearings; and an administrative support staff of four. There is a particular burden on the Committee's administrative support because the material handled by the Committee is sensitive and highly classified, and must be dealt with using special security procedures.

The Committee decides formally at its monthly meetings the research and other activities it wishes to pursue, and sets priorities for the staff. Day-to-day operations are delegated to the Executive Director with direction, where necessary, from the Chairman in his role as the Chief Executive Officer of the organization.

Appendices

A. Glossary

CASIS — Canadian Association for Security and Intelligence Study

CEIC — Canadian Employment and Immigration Commission

CI — Counter-Intelligence

COMMITTEE — Security Intelligence Review Committee (SIRC)

CPIC — Canadian Police Information Centre

CSE — Communications Security Establishment

CSIS — Canadian Security Intelligence Service

CT — Counter-Terrorism

DIRECTOR — the Director of CSIS

DND — Department of National Defence

GSP — Government Security Policy

HQ — Headquarters

IO — Intelligence Officer

IPC — Intelligence Production Committee

MEK — Mujahedin-E-Khalq

MINISTER — the Solicitor General of Canada, unless otherwise stated

MOU — Memorandum of Understanding

OM — Operational Manual

RAP — Requirements Analysis and Production Branch

RCMP — Royal Canadian Mounted Police

RDP — Refugee Determination Program

R & D — Research and Development

RTT — Requirements-Technology Transfer

S & T — Science and Technology

SERVICE — Canadian Security Intelligence Service (CSIS)

SIRC — Security Intelligence Review Committee

SIU — Special Investigation Unit (DND)

SLO — Security Liaison Officer

TARC — Targeting Approval and Review Committee

US — United States

WMD — Weapons of Mass Destruction

B. SIRC Reports and Studies since 1984

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

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

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

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

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

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

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

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

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

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

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

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

Supplement to the Committee's Report on Immigration Screening of January 18, 1988, 15 November 1989 (SECRET) ***** (89/90-01)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Domestic Terrorism Targets — A SIRC Review, July 92 (TOP SECRET) ***** (90/91-13)

Review of CSIS Investigation of a Latin American Illegal, November 92 (TOP SECRET) ***** (90/91-10)

CSIS Activities in regard to the destruction of Air India Flight 182 on June 23, 1985 — A SIRC Review, November 92 (TOP SECRET) ***** (91/92-14)

Prairie Region — Report on Targeting Authorizations (Chapter 1), November 92 (TOP SECRET) ***** (90/91-11)

CSIS Activities during the Gulf War: Community Interviews, September 92 (SECRET) (90/91-12)

The Audit of Section 16 Investigations, September 92 (TOP SECRET) (91/92-18)

Prairie Region Audit, January 93 (TOP SECRET) (90/91-11)

``STUDYNT'' The Second CSIS Internal Security Case, May 92 (TOP SECRET) (91/92-15)

The Assault on Dr. Hassan AL-TURABI, November 92 (SECRET) (92/93-07)

CSIS Activities with respect to Citizenship Security Screening, July 92 (SECRET) (91/92-12)

Domestic Exchanges of Information (A SIRC Review — 1991/92), November 92 (SECRET) (91/92-16)

Counter-Terrorism Study 93-04, December 1993 (SECRET) *****

Counter-Intelligence Study 93-05, December 1993 (SECRET)

Counter-Terrorism Study 93-06, May 1993 (SECRET)

Counter-Terrorism Study 93-03, September 1993 (SECRET)

Regional Audit, September 1993 (TOP SECRET)

Counter-Intelligence Study 93-03, November 1993 (TOP SECRET)

Counter-Intelligence Study 93-04, December 1993 (SECRET)

Counter-Terrorism Study 93-01, December 1993 (SECRET)

Counter-Terrorism Study 93-02, December 1993 (SECRET)

Counter-Intelligence Study 93-01, December 1993 (TOP SECRET)

Counter-Intelligence Study 93-11, May 1994 (TOP SECRET)

C. Complaints Case Histories

Security Clearance — Case 1

The individual, formerly employed with the Department of National Defence, complained about the Department's downgrading of a security clearance. Due to the downgrade from a Level 3 to a Level 1 clearance, the individual was forced to resign from the Department, and appealed the decision to SIRC.

The complainant subsequently withdrew the complaint, and so the Review Committee was unable to complete the investigation.

Security Clearance — Case 2

The security clearance of a CSIS employee was revoked after CSIS concluded that the person's behaviour was unsuitable for a CSIS employee.

The Committee concluded that the complainant's behaviour had been unsuitable for several years. The Committee also concluded that the Service should have dealt with the situation very much earlier.

Undue Delay — Case 3

The complainant expressed concern about CSIS' delay in processing an application for permanent resident status.

The Committee concluded that the internal organization of the Security Screening Branch, and some aspects of the security screening procedures in place during the processing of the complainant's application, left a great deal to be desired.

However, the Committee concluded that the complainant was not, in fact, unduly prejudiced by delay.

Community Interviews — Case 4

An individual complained after being interviewed twice by CSIS for the purpose of ``community interviews." The complainant sought clarification as to the authority under which the interviews were conducted.

The Committee concluded that two interviews complied with legislation, Ministerial direction and the Service's policy and procedures. However, the Committee also concluded that the actions of CSIS investigators in this case were not beyond reproach.

Security Clearance — Case 5

This case involved two separate complaints.

One complaint related to a security screening investigation that happened over ten years ago under the jurisdiction of the RCMP. Since the Committee only has authority to investigate ``any act or thing done by the Service" since June 16, 1984, and because the file had been destroyed, we declined jurisdiction for the first investigation.

The second complaint dealt with the length of time taken by the Service in providing advice, and the accuracy of comments made by people interviewed in the course of the Service's investigation.

We fully investigated the 1988 security screening investigation by the Service.

The Committee concluded that it could not support this complaint because the Service had, in fact, recommended that the complainant be granted a security clearance.

Request for Additional Compensation — Case 6

The complainant, who was a long standing human source of the RCMP and then CSIS, believed he was entitled to additional compensation.

The Committee did not have jurisdiction to investigate activities which took place prior to July 16, 1984. However, because the complainant's grievance also covered several years after that date, the Committee conducted a full investigation.

The Committee decided that the complainant was treated ethically and fairly in terms of compensation and of severance payments. The Committee also concluded that the complainant had no right to additional compensation.

Security Impediment — Case 7

An individual submitted a complaint, ``in order to have removed the security impediment to the processing of a Russian national for permanent residence." Our mandate in this case was to decide whether the Service's activities in providing security advice to the Department of Citizenship and Immigration were properly and adequately carried out.

The Committee concluded that it did not have any recommendation to make since the complaint was not supported in any way by the evidence.

Security Breaches — Case 8

The complainant alleged that there were security lapses within a section of the Service.

The Committee concluded that there were security problems in that Section and that CSIS had subsequently taken adequate steps to redress the problems revealed by the investigation.

Service Irregularities — Case 9

An individual complained that the Service had terminated a security clearance investigation despite the fact that a number of irregularities had been discovered which had not been resolved.

The Committee recommended that the Director of CSIS reopen the investigation with a view to resolving some of the concerns raised in the complaint.