



SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# SIRC Report 2002-2003

An Operational Review of the  
Canadian Security Intelligence Service

Canada





SECURITY INTELLIGENCE  
REVIEW COMMITTEE

# **SIRC Report 2002–2003**

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

Security Intelligence Review Committee  
P.O. Box 2430, Station "D"  
Ottawa ON  
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

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

Collect calls are accepted between 8:00 a.m. and 5:00 p.m. Eastern Standard Time.

© Public Works and Government Services Canada 2003

Cat. No. JS71-1/2003

ISBN 0-662-67626-2

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

September 30, 2003

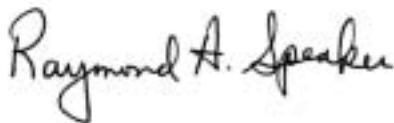
Dear Mr. Easter:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2002–2003, for your submission to Parliament.

Yours sincerely,



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



Raymond Speaker, P.C., O.C.



Gary Filmon, P.C., O.M.



Baljit S. Chadha, P.C.



## Contents

---

Statement from the Committee .....	vii
How SIRC’s Report is Organized .....	x
<b>Section 1: SIRC Review and Complaints Functions .....</b>	<b>1</b>
<b>A. Reviews of CSIS Security Intelligence Activities .....</b>	<b>3</b>
How SIRC Carries Out its Review Function—An Overview .....	3
In the Matter of Ahmed Ressam .....	5
Sunni Islamic Extremism—A Review of CSIS	
Regional Investigations .....	7
Domestic Threats in Conjunction with Lawful Advocacy,	
Protest and Dissent .....	14
Collection of Foreign Intelligence .....	18
Review of Foreign Arrangements .....	21
<b>B. Investigations of Complaints .....</b>	<b>23</b>
Reports of Decisions—Case Histories .....	24
Section 41—“Any act or thing” .....	24
Section 42—Denial of Security Clearance .....	27
<b>C. Section 54 Report to the Solicitor General</b>	
<b>Respecting Allegations of CSIS Misconduct .....</b>	<b>28</b>
<b>Section 2: CSIS Accountability Mechanisms .....</b>	<b>29</b>
<b>A. Policy And Governance Framework .....</b>	<b>31</b>
2002–2003 National Requirements for Security Intelligence .....	31

Ministerial Direction . . . . .	31
Governor in Council Regulations and Appointments . . . . .	31
Section 28 Regulations . . . . .	32
Changes in CSIS Operational Policy . . . . .	32
<b>B. Reporting Requirements . . . . .</b>	<b>33</b>
Certificate of the Inspector General for 2002 . . . . .	33
CSIS Annual Operational Report for 2001–2002 . . . . .	34
Unlawful Conduct . . . . .	34
Section 2(d) Investigations . . . . .	34
Disclosures of Information in the Public or National Interest . . . . .	35
<b>C. CSIS Operational Activities . . . . .</b>	<b>35</b>
Counter Proliferation . . . . .	35
Counter Terrorism . . . . .	36
Counter Intelligence . . . . .	37
Research, Analysis and Production . . . . .	37
Security Screening . . . . .	38
CSIS Domestic and International Arrangements . . . . .	43
Federal Court Warrants and Warrant Statistics . . . . .	45
<b>Section 3: Inside The Security Intelligence</b>	
<b>Review Committee . . . . .</b>	<b>47</b>
Appointment of a New Member . . . . .	49
Senior Staff Appointments at SIRC . . . . .	49
SIRC Staffing and Organization . . . . .	49
Research and Review Activities . . . . .	50
Security Intelligence Briefings . . . . .	50
Parliamentary Relations . . . . .	50
Additional Committee Activities . . . . .	50
Budget and Expenditures . . . . .	51
SIRC Request for Increased Funding . . . . .	51
Inquiries Under the Access to Information and Privacy Acts . . . . .	52
<b>Appendix A: Acronyms . . . . .</b>	<b>53</b>
<b>Appendix B: SIRC Reports and Studies since 1984 . . . . .</b>	<b>57</b>
<b>Appendix C: Key Findings and Recommendations . . . . .</b>	<b>69</b>

## Statement from the Committee

---

Canada's security intelligence and public security apparatus continues to absorb the repercussions of the terrorist attacks of September 11, 2001. For the security intelligence community generally, and for the Review Committee in particular, some of the most important of these are only now being fully realized.

SIRC's Annual Report for 2002–2003 encompasses the first year in which significant new laws, the *Anti-terrorism Act* among others, were in force. It was also the first complete fiscal year in which Canadian citizens fully felt in their lives measures announced in the Government's public safety and security initiative of December 2001. These measures have affected everything from passing through an airport or working in one, to applying for a passport and holding a job in a nuclear power facility. Dramatic political and military events abroad—some involving serious risk to the lives of Canadian citizens and to Canada's soldiers overseas—could not help but have consequences within our borders.

In this dynamic domestic and international environment, the Review Committee must reconcile two distinct imperatives. Parliament has every right to expect, and simple professional prudence requires, that the Committee understands as best it can the changes at work and the impact they are having or may have on CSIS's activities. To this end, the Members of the Committee devote considerable effort.

At the same time, however, the Committee is convinced that continuity of principle and of practice is central to our task. Adherence to the law, sober judgement and serious inquiry—irrespective of the political and social undercurrents of the moment—are the Committee's main assets in fulfilling its core function: ensuring Parliament, and through it the people of Canada, that in conducting its security intelligence activities CSIS acts within the law and does not undermine the rights and freedoms of Canadians.



The period encompassed in this, the Committee's 19th Annual Report, was the first complete fiscal year in which CSIS had at its disposal the 30-percent increase in funding given to it by the Government following September 11. Although the Service was given no new legal authorities, the tempo of activity in many operational areas has risen—in some cases significantly.

CSIS reorganized its operational structure and began to deploy resources in novel ways. For example, Service personnel and resources are devoted both to new government efforts to coordinate its anti-terrorist and public safety programs such as the public-private CBRN Research and Technology Initiative that addresses threats from chemical, biological, radiological and nuclear weapons, and to the RCMP's regionally based Integrated National Security Enforcement Teams (INSETs).

Almost all this heightened level of activity can be attributed to the Government's concern to meet evident threats to the safety of its citizens, to Canada's national security and to that of its allies.

As the Service's investigations become more numerous and complex, there is more for the Committee to review.

However, with higher levels of activity there is an inescapable reality—as the Service's investigations become more numerous and complex, there is more for the Committee to review.

In the spring of 2002, we undertook to assess the implications of the rise in CSIS activities for SIRC's own operations. We asked for and received two classified briefings from the Service about how it intended to use the additional funds. Accordingly, in July 2002 SIRC made a formal request to Treasury Board for an increase in budget of 16 percent. If granted, this increment would provide the Committee with the financial resources commensurate with CSIS's expanded activities so that we might continue to fulfill our obligations to Parliament.

An additional challenge the Committee faces is that the Service is stepping up its co-operation and information exchanges both with old partners in new ways and with entirely new entities. As the Service moves into new and unfamiliar territory, so must the Committee. An example of the potential challenges to be found in such relationships are the RCMP-led INSETs created in 2002, and the reciprocal secondments of officers initiated between CSIS and the RCMP. Under this structure—one that replaces the long-standing mutual exchange of "liaison officers"—investigative personnel from each agency will work within the chain of command of the host body.

The Committee has some misgivings about the impact of this new structure on our ability to determine whether the Service and its employees have acted in compliance with current law and policy. As the Service expands its operational relationships with organizations not subject to the Committee's review, the Committee will remain alert to the compliance issues this and other such novel arrangements might raise.

One prediction the Committee made based on an analysis of the post-September 11 changes in legislation—notably the *Anti-terrorism Act*, the *Immigration and Refugee Protection Act* and the *Charities Registration Act*—has not been borne out. In recent SIRC Annual Reports, and in representations to Parliament, the Committee forecast that complaints about CSIS would increase discernibly, especially in areas of security screening and charities. However, the anticipated rise in the number of complaints has not occurred.

No doubt one factor at work is the relative caution with which the Government has implemented the new legal and administrative measures. There has been no significant increase in the number of arrests or detentions on terrorism or immigration-related charges. The “listing” of terrorist entities has proceeded largely without controversy. And to date, no charities have been denied status or had it withdrawn because of ties to known terrorist organizations.

Findings in two of the Committee's in-depth reviews summarized in this report tend to support this observation. In its investigation of certain potentially violent domestic threats the Service took care not to impede legitimate political activity. In its investigations of Islamic extremist terrorism in Canada, the Service restricted its activities to the threats posed by persons and organizations disposed to employ violence and did not investigate the Islamic community as a whole. The broadly positive findings of these two reviews notwithstanding, the Committee will continue to pay its closest attention to any Service investigation that holds the potential to damage civil liberties or to impact negatively on fundamental social institutions such as religious organizations, universities, the media and trade unions.

It is this latter task which the Committee sees as its chief function. For CSIS to be effective in advising government about threats to the security of Canada and its citizens, Parliament and the people of Canada must have confidence that it is acting within the law. The Review Committee is the essential component in ensuring that vital democratic accountability. Within the boundaries set by law on the public discussion of security intelligence issues, the Members of the Review Committee undertake, as always, to be as open and transparent with Parliament and the public as we are able.

## How SIRC's Report is Organized

The organization of the 2002–2003 Annual Report differs slightly from that of previous years—modified so that readers can more readily identify important Review Committee findings and understand the nature of the information being presented.

**Section 1: SIRC Review and Complaints Functions** encompasses all findings and recommendations arising out of specific reviews of CSIS activities undertaken by the Committee, and all observations and conclusions arising from SIRC investigations of individual complaints about the Service during the period covered by the report.

**Section 2: CSIS Accountability Mechanisms** has two purposes: first, to present relevant contextual information about those elements of Canada's security intelligence governance system that inform the legal and policy framework in which CSIS and SIRC carry out their respective mandates, and second, to summarize information provided to the Committee by the Service about changes in its operational plans and priorities.

**Section 3: Inside the Security Intelligence Review Committee** reviews the information gathering, outreach and administrative activities of the Committee itself—appointments of Committee Members and the Committee's annual budget and expenditures are chief among subjects discussed.

As with all SIRC Annual Reports in recent years, the format of the report throughout draws a clear distinction between Committee findings, observations and recommendations derived from Committee investigations, and more general background material designed to assist readers in understanding the broader context in which security and intelligence work is carried out.

Subjects that the Committee believes will be of background, historical or technical interest to readers are set apart from the main text in shaded insets. They do not reflect Committee opinions or conclusions and are intended to be factual in nature.

## **Section 1**

---

### **SIRC Review and Complaints Functions**



## SIRC Review and Complaints Functions

### A. Reviews of CSIS Security Intelligence Activities

#### How SIRC Carries Out Its Review Function— An Overview

##### **THE COMMITTEE'S ROLE IN CSIS'S ACCOUNTABILITY STRUCTURE**

A significant component of SIRC's review activity takes the form of research projects carried out by staff, directed by Committee Members. As a matter of policy, and in accordance with the Committee's role in the Service's governance and accountability structure, the Committee reviews CSIS's performance of its duties and functions retrospectively to assure itself—and, by extension, Parliament and the people of Canada—that the Service has acted appropriately and within the law.

The Service continues at all times to be accountable for current operations through the existing apparatus of government, specifically the Ministry of the Solicitor General and the Office of the Inspector General of CSIS. With respect to its financial administration, CSIS, like almost all federal bodies, is responsible to government through a Minister of the Crown (in the Service's case, the Solicitor General), the central agencies of government and directly to Parliament through the Office of the Auditor General of Canada.

##### **THE FOCUS OF SIRC STUDIES—CHOICES AND RESPONSIBILITIES**

The Committee's review function is essentially one of risk management. It decides which areas of the Service's extensive operational activities warrant the most careful monitoring. The content of any individual study and its findings arise from examining the relevant documents and interviewing individuals who are pertinent to that study. The findings of any single review are not to be read as a judgment on the Service's operations as a whole.

SIRC research projects for any given year are designed to yield assessments across the range of CSIS's operational activities. This approach helps ensure that, over time, the Committee comes to understand comprehensively the Service's activities and is thus able to either assure Parliament that the Service has acted appropriately, or to inform Parliament in a timely and instructive manner that it has not.

A number of factors influence which topics are selected for in-depth inquiry:

- the nature of the international threat environment;
- public undertakings by the Committee to follow up on past reviews or to launch new ones;
- issues arising from complaints brought before the Committee;
- alterations in government policy or practice with significant implications for CSIS operations; and
- SIRC's statutory obligations under section 38 of the *CSIS Act*.

The selection of topics for review is approved by the Committee at the beginning of each fiscal year. However, the Committee has the capacity to adjust its review plans to respond to unexpected events and has done so on several occasions.

### **SIRC REVIEWS IN 2002–2003**

Several of the factors listed above worked to determine which reviews were selected for 2002–2003. With our report on CSIS's investigation into Sunni Islamic extremism in two regions, the Committee fulfills a commitment made in last year's Annual Report to follow up on its foundation study of this complex area. Similarly, our review of the Ahmed Ressam matter completes a public undertaking the Committee made early in 2001 to look into the case at a later date.

The Committee has the capacity to adjust its review plans to respond to unexpected events.

The Committee's report on certain domestic threats reflects our continued special interest in any Service operation that has the potential to impact upon lawful advocacy, protest and dissent. Finally, examinations of several CSIS

arrangements with foreign intelligence services, and our study of the Service's role in collecting foreign intelligence in Canada, both speak to another essential element in the Committee's strategy—the regular monitoring of the Service's important operational activities and the execution of our obligations under section 38 of the Act.

Readers will also note that three of the five reports deal with matters of terrorism or politically motivated violence. As we have noted in previous Annual Reports, the Service's chief preoccupation since the mid-1990s has been with threats to public safety posed by terrorism and other forms of serious violence. As CSIS devotes an ever-growing share of its investigative resources to dealing with such threats, the Committee has adjusted its own focus accordingly.

## In the Matter of Ahmed Ressam

---

### Report # 2002-03

---

#### **BACKGROUND**

On December 14, 1999, Ahmed Ressam was arrested while attempting to enter the United States from Canada with explosives hidden in the trunk of his rental car. Ressam was subsequently convicted on charges related to his unsuccessful attempt to carry out a terrorist attack at the Los Angeles International Airport to mark the beginning of the new millennium. Ressam's case attracted intense media coverage and contributed to a perception that Canada was a "safe haven" for terrorists to plan and undertake attacks against the United States.

Following these events, the Review Committee made a public commitment to examine the actions of the Service in respect of Ahmed Ressam at a future date. This report summarizes the Committee's findings and conclusions in the matter.

#### **METHODOLOGY OF THE REVIEW**

The objective of the review was to examine CSIS's investigation of the threat posed by Ressam within the context of Sunni Islamic extremism. As in all Committee reviews, our goal was to ensure that the Service's activities complied with the law, ministerial direction and operational policy.

The review covered the period from Ressam's arrival in Canada in February 1994 through March 31, 2001 and included all relevant Service documents and files (electronic and hard-copy). To complete its inquiries, the Committee examined, as necessary, additional material falling outside this period.

The Committee hoped to answer five key questions:

- 1) What was the nature and the extent of the Service's knowledge of Ressam prior to his arrest?
- 2) What was the substance of the Service's co-operation and exchange of information with domestic and foreign agencies regarding Ressam?
- 3) How did the Service's operational interest in Ressam change following his arrest?



- 4) What was the substance and value of the information CSIS received from United States authorities arising from Ressam's agreement to co-operate with American authorities?
- 5) Did the Ressam matter prompt any changes in CSIS policy or operational practice?

## FINDINGS OF THE COMMITTEE

### CSIS's Knowledge of Ressam Prior to his Arrest

Ahmed Ressam first came to the Service's attention as a result of his contacts with persons suspected of engaging in threat-related activities. During this period CSIS did not regard Ressam's activities in themselves as a threat to the security of Canada. In 1998 the Service learned that Ressam had departed Canada to attend a paramilitary training camp in Afghanistan.

Prior to his departure in 1998, Ressam successfully exploited weaknesses in the Canadian passport application process (since altered), enabling him to obtain a

Actions CSIS took to locate Ressam in 1999 were appropriate in light of information available at the time.

genuine Canadian passport bearing the pseudonym "Benni Antoine Norris." Returning to Canada in February 1999 using this passport, Ressam's re-entry went undetected at the time by Canadian authorities. Sometime later, the Service received

unsubstantiated information that Ressam had returned to Canada. However, his whereabouts and activities remained unknown to the Service until his arrest by U.S. authorities on December 14, 1999.

Upon reviewing all the relevant documentation, the Committee concluded that the Service did not possess specific information that would have forewarned it of Ressam's planned terrorist operations. In the Committee's view, the actions CSIS took to locate Ressam in 1999 were appropriate in light of the information available at the time. The Committee saw no evidence that it was a lack of vigilance on the part of the Service that contributed to Ressam's ability to escape detection after his return in 1999.

### CSIS Activities Post-Arrest

In late 1999 the Service and its partner agencies, both domestic and foreign, were in a heightened state of alert, working actively to identify and disrupt terrorist operations possibly being planned for the turn of the millennium. These efforts became both more intense and more focused after Ressam's arrest in December.

The Committee found that the Service's investigative activities following Ressam's arrest were appropriate and proportionate to the threat. The Service complied with the requirements of law, ministerial direction and policy. All the information collected was strictly necessary to its investigation of an imminent threat to the security of Canada.

All information exchanges between the Service and the RCMP on the Ressam matter were appropriate and, in general, both timely and thorough. This case showed the capacity of the Service and the RCMP to assist each other effectively while working within their respective mandates. Similarly, the exchanges of information between the Service and its U.S. partners were timely and comprehensive, indicating a smooth-functioning and productive relationship.

These events have influenced the Service's methods respecting the Sunni Islamic extremist threat.

#### **Intelligence Gathered from Ressam Post-arrest**

Shortly after his conviction in April 2001, Ressam signed an agreement to co-operate with U.S. authorities in exchange for a reduction of his sentence to a minimum of 27 years' imprisonment. Ressam agreed to participate in detailed debriefings by intelligence officers and to provide testimony in future terrorism-related criminal proceedings. The Service briefed the Committee on the information provided by Ressam and on its utility.

The Service also briefed the Committee on the lessons it drew from the Ressam case—lessons that, for reasons of national security, cannot be discussed in detail here. Although CSIS did not believe changes to operational policy were necessary, these events have influenced the Service's methods respecting an overall approach to the Sunni Islamic extremist threat.

## **Sunni Islamic Extremism—A Review of CSIS Regional Investigations**

---

### **Report #2002-05**

---

#### **BACKGROUND**

Following the events of September 11, 2001 the Review Committee launched a broad-based study into CSIS's investigation prior to the terrorist attacks of the Al Qaida organization and Sunni Islamic extremism generally. Our findings were presented in last year's Annual Report to Parliament.

As the Committee stated at the time, the goal of the study was to lay the foundation for additional focused reviews of specific elements of the Service's long-standing investigation of Sunni Islamic extremism and its connections to terrorism. Presented here are findings from one such in-depth review.

Based on information gathered from the initial survey study, the Committee elected to examine in depth a complex set of related CSIS investigations into Sunni extremism managed from two separate CSIS regional offices during the period April 2001 through March 2002. The regions were selected because among the Service's regional offices, these two were mounting the most intense counter-terrorist investigations of the Sunni extremist threat, thus providing the Committee with the greatest range of CSIS activities to observe.

Besides providing perspective on the Service's conduct of its Sunni Islamic extremist investigation, the Committee's experience is that comprehensive examinations of

Comprehensive examinations of CSIS regional office activities produce unique insights.

CSIS regional office activities produce unique insights into how the Service employs the range of investigative tools it has at its disposal. Taken together, the actions of targeting, acquiring and implementing warrants, conducting interviews in communities, exchanging

information with law enforcement and other intelligence agencies, and handling human sources are the quintessence of counter-terrorist intelligence work.

Understanding these activities allows the Committee to assess the manner in which ministerial direction and CSIS operational policies are being implemented by those sections of CSIS employing the most powerful and intrusive instruments available to government.

#### **METHODOLOGY OF THE REVIEW**

The Committee examined all electronic and hard-copy documentation during the review period related to five broad operational activities:

- 1) the targeting request and approval process, and the investigating of targets;
- 2) the acquiring and implementing of warrants;
- 3) the recruiting, developing and directing of human sources;
- 4) the conducting of interviews in the community; and
- 5) the exchanging of information and other forms of liaison with domestic agencies.

In addition, the Committee visited the regional offices under review and conducted on-site interviews of CSIS senior management.

As in all its reviews of CSIS investigations, the Committee weighed several essential questions in assessing the appropriateness of the Service's activities:

- Did the Service have reasonable grounds to suspect a threat to the security of Canada?
- Was the level and intrusiveness of the investigation proportionate to the seriousness and imminence of the threat?
- Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?

Although not related directly to the Service's Sunni extremism investigation, the Committee also took the opportunity to review each regional office's internal security procedures and any associated issues.

## FINDINGS OF THE COMMITTEE

### Targeting and Investigations

The Committee selected a sample of targets to examine in detail, a selection determined by the relatively high level of investigative activity for each. The Committee found that in all cases the Service had reasonable grounds to suspect the target's involvement in activities that constituted a threat to the security of Canada and that the levels of investigation were proportionate to the threat activities observed.

Two instances drew the Committee's attention and required additional inquiries of the Service.

In obtaining targeting authorities and conducting the investigations, the Service met all the requirements set out in law, ministerial direction and operational policy. It collected only the information strictly necessary for the investigation.

Two instances drew the Committee's attention and required additional inquiries of the Service. In the first, the Committee reviewed documentation about an unusual event involving one of the selected targets. Upon receipt of additional information from the Service, the Committee was satisfied that no improper conduct on the part of CSIS contributed to the event, nor did any Service employee contravene operational policy.

The second instance related to an error on the part of the Service that had been rectified by CSIS as soon as it was noticed. This error involved an instance of mistaken identity. Unusual and extenuating circumstances contributed to the error and the Committee is satisfied that it was unintentional. Further, the Committee was able to confirm that the Service took the proper administrative and operational measures to correct the error as soon as it became evident. The Committee believes that the authorities subsequently invoked by the Service were appropriate.

### **Warrant Acquisition and Implementation**

Under section 21 of the *CSIS Act*, only the Federal Court of Canada can grant CSIS the warrant powers required to exercise its most intrusive investigative techniques, such as telephone or mail intercepts. To obtain such powers, the Service must present an affidavit to the Court attesting to the facts that require their use.

A most critical time—the months immediately before and immediately following the events of September 11, 2001.

In this section of the review the Committee examined the procedures by which Headquarters obtained warrant powers against the selected targets, as well as the procedures followed by the Regions in executing

those powers. By selecting for review those warrants specifically related to the targets, the Committee hoped to gain a more comprehensive understanding of the Service's approach to the Sunni Islamic extremist investigation at a most critical time—the months immediately before and immediately following the events of September 11, 2001.

With respect to all the warrants examined in both regions and based on the information made available to the Committee for review, we found that CSIS conducted the warrant acquisition process in a thorough and objective manner and used supporting information appropriately. Affidavits were complete and balanced, and the facts and circumstances of the cases were fully, fairly and objectively expressed.

In one of the affidavits reviewed, the Committee identified two minor errors and inconsistencies. In the Committee's view, however, these did not materially affect the validity of the cases presented to the Federal Court.

In another affidavit reviewed, an instance of mistaken identity resulted in a similar error in the use of warrant powers. Once the Service investigators recognized

their mistake, CSIS returned to the Federal Court with a new affidavit and the Court issued a supplemental warrant.

The Committee also found that in executing the warrant powers obtained, CSIS exercised its powers appropriately and complied with all warrant clauses and conditions. With minor exceptions, both regions strictly observed operational policies concerning the collection and retention of information obtained under the warrants. In one Region, however, the Committee identified administrative errors in the recording of information emanating from warrant powers. We drew the Service's attention to these lapses in accuracy.

### **Recruitment and Direction of Human Sources**

The use of human sources to collect information is essential to the Service's effective investigation of threats to public safety and national security. However, the sensitivity of such operations is such that they are the subject of special ministerial direction and detailed operational policy. All requests by CSIS investigators to employ human sources, which impact or appear to impact on "sensitive" or "fundamental" institutions (generally defined as trade unions, the media, religious institutions and university and college campuses) require the approval of CSIS senior management or, in some cases, the Solicitor General.

The Committee selected for review a number of human source cases associated with the Sunni extremist investigation in the two regions. We examined all relevant files and logs, and all notifications and requests for approval related to sensitive institutions.

In all cases the Committee found that the Service had acted appropriately and within the law and had properly followed all policies and procedures relating to the recruiting and directing of human sources. In one especially sensitive area of the Service's use of human sources—one that had drawn the Committee's attention previously (*see* SIRC Report 2001–2002, page 8)—the Committee found that CSIS managed the relationship with the source appropriately.

The Committee did identify some minor errors and oversights in one Region's human source record keeping. Although the Committee does not believe these lapses were representative of the overall high quality of CSIS's management of the human source cases reviewed, the importance of proper documentation to human source operations generally required that we bring even these relatively minor administrative errors to the attention of the Service.

### Interviews in the Community

To aid an investigation, CSIS may conduct interviews with leaders of communities or interest groups concerning threats to the security of Canada that may affect their communities. There is specific operational policy guidance for such interviews: Service employees must clearly identify themselves as such, the interviewee must be made aware that co-operation is voluntary, and the interviews must be carried out in such a way that it is clear that it is a threat that is being investigated, not the community itself.

In determining whether these interviews were conducted appropriately, the Committee examined the stated rationale for conducting the interviews, CSIS

The sensitivity of such operations is such that they are the subject of special ministerial direction.

reporting on both the content of the interviews and the manner in which they were conducted, and the extent to which the interviews may have aided or impeded the Service's investigations into Sunni Islamic extremism.

The Committee's review of relevant CSIS documentation showed that it conducted its interviews in a fair and appropriate manner and with sensitivity to the interviewees' civil liberties and religious freedoms. In all the interviews reviewed, CSIS was careful to make interviewees aware that it was investigating threats posed by Sunni Islamic extremism, not investigating the Sunni community as a whole. The Committee also concluded that the interviews were of operational assistance to the Service in identifying specific threats to public safety and national security.

### Liaison and Exchanges of Information with Domestic Agencies

The Committee examined all relevant information regarding liaison and co-operation between the Service and other domestic agencies that pertained to the targets under review. Included in this documentation were all logged exchanges of intelligence with other domestic agencies related to those targets. The Committee was especially concerned to determine whether co-operation was timely, effective and in conformity with law, ministerial direction and operational policy.

The Committee's examination showed that all exchanges of information, disclosures by the Service and joint operations were conducted in accordance with law and policy. The Service's efforts in both Regions to build strong and co-operative relationships with other agencies were evident to the Committee. In the months following the September 11 attacks, the benefit of these initiatives was especially important because available resources to investigate threats were stretched thin.

The Service's relations with the RCMP have been of long-standing interest to the Committee. Based on our review of the two regions in question, the Service's Sunni Islamic extremist investigations benefited from an effective working relationship between the two agencies.

### Issues of Internal Security

Internal security issues are an integral part of any Committee review of a Service regional office. In assessing the adequacy of security practices and procedures, the Committee can observe how operational policies, developed centrally, are implemented in the field. In the event of security violations or more seriously, security breaches, the Committee requests a follow-up from the Service so it can determine whether these have been addressed satisfactorily. The Committee's review of internal security covers the period since our last review.

Internal security issues are a part of any Committee review of a regional office.

In one region, the Committee identified a number of security violations and no breaches.\* The Region took remedial action in the form of security training sessions whose aim was to re-sensitize employees to the need for strict adherence to security procedures.

In the other region, the Service had documented five security breaches: one unauthorized contact, one conflict of interest situation and three involving unauthorized disclosures. In four of the cases the Committee agreed with the measures CSIS took to mitigate possible impacts from the breaches and found that the administrative measures the Service took in relation to the employees concerned were appropriate. The fifth case remains under review by the Committee.

### CONCLUSIONS

The investigations reviewed here straddle the months before and after the events of September 11, 2001. It was evident to the Committee that the Service's investigations of Sunni Islamic extremism in general, and the specific targets we examined, were well underway before September 11. The Service had identified targets, sought and obtained warrant powers, developed useful human sources

---

\* CSIS operational policy defines a security violation as any contravention of Service security policies or procedures, for example, the failure to lock up or otherwise physically secure classified information. A security breach is deemed to have occurred when any classified or designated information or asset is the subject of unauthorized access or disclosure.



and had regular and extensive exchanges of information with other relevant Canadian agencies.

The events of September 11 certainly intensified the Service's own activities and the level of exchanges with other agencies. However, the nature and intent of the

Efforts to build strong and co-operative relationships with other agencies were evident to the Committee.

overall investigation did not change.

Before and after September 11 the Service's investigations in both regions appeared to the Committee to be thorough, well managed and appropriately documented. Rules and procedures designed to protect individual civil

liberties and religious and social institutions were scrupulously observed throughout. The Committee identified no evidence or information that would indicate that CSIS had in its possession any information that should have alerted it, and through it the Government, to the impending events of September 11.

## Domestic Threats in Conjunction with Lawful Advocacy, Protest and Dissent

### Report #2002-04

#### BACKGROUND

Historically, the Committee has taken special interest in Service investigations involving threat-related activities that occur at the same time or in the same location as legitimate political advocacy and dissent. It is here where the national security imperative to use intrusive investigative techniques must be weighed most carefully against potential damage to individual rights and fundamental institutions. Invariably, such investigations are sensitive and complex, circumstances in which the Committee is especially concerned to ensure that the Service is complying fully with existing law and policy.

#### SCOPE AND METHODOLOGY OF THE REVIEW

The purpose of this study was to examine CSIS's investigation of groups and individuals whose activities were suspected of being directed towards threats of serious violence while in the course of advocating for or protesting about issues of social and economic concern. The Committee reviewed Service investigations of 13 targets: 2 issue/events-based targets, 3 organizations and 8 individuals. The Committee reviewed all relevant Service documentation and information (both electronic and hard-copy) for the period April 1, 2000 through June 30, 2002.

## Lawful Advocacy, Protest and Dissent

CSIS is prohibited from investigating activities involving lawful advocacy, protest and dissent unless they occur in conjunction with threats to the security of Canada as defined in the *CSIS Act*. Even then, safeguards are in place to prevent unwarranted intrusion by the Service into the legitimate political activities of Canadians. In all cases, CSIS is obliged to weigh the use of intrusive investigative techniques against possible damage to civil liberties or fundamental social institutions.

Ministerial direction and several key operational policies direct the Service to follow specific measures when there is a risk its actions may impinge on either legitimate political activity or on fundamental societal institutions that depend on individual rights and freedoms to function effectively. Pre-eminent among these institutions are those in academic, religious, media and trade union fields.

Although there are no sanctuaries from lawful and authorized investigations into threats to the security of Canada, CSIS investigations associated with fundamental institutions are subject to policies more stringent than most other areas of Service operations.

The scope of CSIS operational activities reviewed was comprehensive. The Committee's examination encompassed the targeting request and approval process; investigations of targets; the implementation of warrant powers and special operations; the recruitment, development, and tasking of human sources; and the nature of co-operative activities within liaison relationships, including exchanges of information with domestic agencies and departments.

For all the investigations reviewed, the Committee needed to assure itself on five essential matters:

- 1) Did the Service have reasonable grounds to suspect a threat to the security of Canada?
- 2) Was the level of investigation proportionate to the seriousness and imminence of the threat?
- 3) Did the Service collect only information strictly necessary to advise the Government of a threat?

- 4) Were the exchanges of information between CSIS and other agencies in conformity with the law, ministerial direction and relevant Memoranda of Understanding (MOUs)?
- 5) In conducting its investigations, did the Service respect the rights and civil liberties of individuals and groups to engage in lawful protest and dissent?

#### **FINDINGS OF THE COMMITTEE**

The Committee found that overall, CSIS conducted this complex set of investigations in an appropriate, lawful and professional manner, taking considerable care in implementing policy measures designed to prevent intrusion into legitimate

political activity. The issue/events-based authorities were implemented judiciously, with the Service seeking identity-based targeting authorities where appropriate in an expeditious manner. The Committee believes, based on its investigation, that the Service

The Committee believes CSIS should have terminated its investigations earlier than it did.

took seriously its obligation to weigh the requirement to protect civil liberties against the need to investigate threats to national security.

For all the targets investigated, the Service had reasonable grounds to suspect a threat, and the level of investigation was in each case proportionate to the nature of the threat. No information that was not strictly necessary to the investigations was collected, and all information exchanges with other agencies were conducted appropriately and within the law.

During the Committee's review of the extensive documentation related to these investigations, the Committee identified a number of issues that gave rise to several recommendations.

#### **Terminating Investigations in a Timely Manner**

Operational policy requires the Service to terminate an investigation—irrespective of the expiry date of the targeting authority—if the activities of the target no longer constitute a threat. In the case of two individual targets where it was clear that threat activities had abated, the Committee believes CSIS should have terminated its investigations earlier than it did. In addition to the general policy guidance, CSIS officers responsible for the investigation received explicit direction from management to end the investigations if no threat activities were reported.

## Issue/Event-based Targeting

This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects that there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not yet been identified. As in any other targeting procedure, if warrant powers are involved, approval must be granted by the Federal Court. Operational policy dictates that as soon as individual persons, groups or organizations are identified as taking part in threat-related activities in connection with an issue or event, the Service will seek separate targeting authority.

On the subject of issue-based targeting, the Committee stated in its 1998–1999 Annual Report that, While there is a place for issue-based targeting in the array of options legally available to CSIS ... investigations under such authorities should be carefully monitored by senior management ... We urge the Service to make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable.

It continues to be the Committee's practice to assess all issue/event-based investigations on a case-by-case basis as we encounter them so as to assure ourselves that they are being conducted appropriately.

To avoid such occurrences in the future, the Committee recommended that:

**CSIS maintain a strict awareness of operational policy and executive directive requiring the timely termination of targeting authorities in the absence of targets' threat-related activity.**

### Implementation of Warrant Powers

In executing valid warrant powers against an individual target, CSIS reported extensively on a non-targeted individual and collected information on that person's threat-related activities without seeking a separate targeting authority. In the Committee's view, the Service should have sought a separate targeting authority rather than rely on another investigation to collect the information it did.

Accordingly, based on this case the Committee recommended that:

**In its collection of information through the execution of warrant powers, CSIS avoid extensive reporting on non-targeted individuals and be vigilant in seeking targeting authority once an individual's threat-related activities become evident.**

### Human Source Operations

In reviewing the Service's conduct of human source operations, the Committee identified several administrative oversights and delays in the Service's handling of a human source file. None had any material impact on the course of the investigation or the information collected. Nevertheless, based on this case the Committee recommended that in future:

**CSIS pay strict attention to operational policy requirements regarding the administrative handling of human source files.**

### Domestic Co-operation and Liaison

The requirement for CSIS to liaise and exchange information with other domestic agencies featured quite prominently in the investigations reviewed. For the most part, these relationships were professional and productive. However, the Committee did find evidence of some friction. This clearly presented challenges but did not, in the Committee's view, materially impact upon the Service's effectiveness in conducting its investigations.

Accordingly, the Committee has recommended to the Service that:

**It examine whether the negotiation of co-operative agreements between CSIS and its domestic partners would be of benefit and enhance their relationships.**

## Collection of Foreign Intelligence

---

### Report #2002-02

---

#### BACKGROUND

Foreign intelligence is defined as any information collected in Canada about the capabilities, intentions or activities of a foreign state, foreign national or foreign organization (including commercial enterprises). Under section 16 of the *CSIS Act*, the Secretary of State for External Affairs—now the Minister of Foreign Affairs—and the Minister of National Defence have the authority to request the assistance of CSIS in collecting foreign intelligence. The Act also expressly directs SIRC to monitor these formal requests for assistance.

#### METHODOLOGY

The Committee's review encompassed all requests for assistance during fiscal year 2001–2002. It included all section 16–derived information retained by CSIS for national security purposes and all exchanges of information with the

## Background to the Collection of Section 16 Foreign Intelligence

### Procedures

Under the provisions of section 16, either the Minister of National Defence or the Minister of Foreign Affairs and International Trade may request “in writing” the assistance of the Service in collecting foreign intelligence. If the Solicitor General agrees with the request, it, along with written concurrence and direction, is passed to the Director of the Service.

CSIS may retain in its section 12 database any foreign intelligence it collects only if it aids investigations falling under section 12 of the *CSIS Act*. The Service acquires foreign intelligence by various means including section 16 activities, CSE-derived material and reporting received from allied agencies.

### Restrictions

The Act specifically prohibits any section 16 collection being directed at Canadian citizens, landed immigrants or Canadian corporations. In the event that CSIS chooses not to retain section 16 information for a section 12 investigation, SIRC’s jurisdiction ends once the material has been provided to the requesting minister. The legislation and related Memoranda of Understanding (MOUs) specifically recognize the Committee’s role in monitoring the Service’s activities in collecting foreign intelligence to ensure, *inter alia*, that intelligence so gathered is not being used in a manner otherwise restricted by the *CSIS Act*.

Information that CSE gives to the Service is routinely “minimized” to comply with various directions governing the prohibition against targeting Canadian nationals and Canadian businesses. Thus, the name of a Canadian person or entity, which had been collected incidentally, would be reported to the Service using language such as “a Canadian person” or “a Canadian company.” Under specific circumstances defined in policy, the Service—if it can demonstrate that the information relates to activities that could constitute a threat to the security of Canada as defined in section 2 of the *CSIS Act*—may request identification from CSE.

### Evolving Nature of Collection Activities

Since 1990, collection activities under section 16 have gradually increased. The Committee believes several factors are behind this trend. First, the notion of collecting foreign intelligence in the early years of the Act was novel and untested. It was only after the signing of the Tri-Ministerial MOU that the details of exactly how to proceed were established. Second, there has been a growing awareness within government of the utility of the kind of information that tasking under section 16 can generate.

Communications Security Establishment (CSE) related to foreign intelligence collection. Given the events of September 11, 2001, the Committee took special care to understand the impact, if any, on the section 16 program.

The goal of the review was to:

- examine CSIS's role in section 16 requests to ensure compliance with the *CSIS Act*, directions from the Federal Court, any related ministerial direction, and the governing 1987 and 1990 MOUs;
- examine the nature of the CSIS/CSE relationship as it relates to section 16 matters to ensure that it complies with the law, ministerial direction and operational policy; and
- understand the impact, if any, on the section 16 program of the terrorist attacks of September 2001.

## **FINDINGS OF THE COMMITTEE**

### **Requests for Assistance**

CSIS's implementation of all ministerial requests under section 16 complied with the necessary legal and administrative requirements.

### **Legislative, Governmental and Judicial Guidance**

The Committee found that for the period under review no new CSIS policies, ministerial directions, judicial instructions or other guidelines were issued that had any impact on the section 16 program.

### **Warrant Implementation**

The Committee reviewed a selection of warrants directed at collecting information under section 16. Our examination encompassed all related working files, affidavits and logs. The review identified no irregularities or other concerns regarding the authorisations for, and the management of, the warranted collection activity.

### **Requests for Identifying Information**

Information that CSE gives to the Service is routinely "minimized" to comply with various directions governing the prohibition against targeting Canadian nationals and Canadian businesses. Under specific circumstances defined in policy, CSIS may request from CSE the identities of Canadians if it can demonstrate that the information relates to activities that could constitute a threat to the security of Canada as defined in section 2 of the *CSIS Act*.

The Committee examined all requests for supplementary information and determined that all were appropriate and in compliance with both law and policy. We saw no information about Canadians collected in the course of operations under section 16 that had been inappropriately retained in Service files.

#### **Access to the Foreign Intelligence Data Base**

Given the extremely sensitive nature of section 16 operations, access to the Foreign Intelligence Data Base is restricted to only those CSIS employees who have received special clearance and indoctrination. The database is thus not routinely accessible to intelligence officers involved in section 12 investigations. The Committee examined a random sample of correspondence related to the indoctrination of section 16 intelligence officers and their requests for access to the database. All requests examined were found to be in compliance with policy.

#### **Impact of the September 11 Terrorist Attacks**

As with most other areas of CSIS operations, the section 16 program came under considerable pressure in the aftermath of the September 11 attacks. There was renewed emphasis on the Service's capacity to coordinate with the other agencies of government involved in the section 16 process.

## **Review of Foreign Arrangements**

### **BACKGROUND**

Under section 17 of the *CSIS Act*, the Service “may enter into an arrangement or otherwise co-operate with” institutions of the government of a foreign country or with an international organization. Such arrangements can only enter into effect after consultation with the Minister of Foreign Affairs and upon the approval of the Solicitor General. Section 38 of the Act directs the Committee to review all such arrangements.

This report encompasses the review of seven arrangements: five were new; two were expanded in scope.

### **METHODOLOGY OF THE REVIEW**

For each arrangement, the Committee examined:

- all relevant information provided to the Solicitor General by the Service;
- all correspondence relating to consultations with the Minister of Foreign Affairs;
- the co-operation file for the foreign agency in question;



- the most recent assessment of the agency in question written by the Security Liaison Officer (SLO) responsible;
- the SLO's overseas post profile; and
- any documentation related to conditions that may have been imposed by the Solicitor General.

### **FINDINGS OF THE COMMITTEE**

Ministerial direction dictates the procedures and conditions necessary to establish a new arrangement or to expand the scope of an existing one. On March 1, 2001 the new compendium of ministerial direction came into effect, somewhat altering the guidelines for administering foreign arrangements generally. The language defining the scope of the arrangements was simplified and certain powers to modify existing relationships were delegated to the Director of CSIS.

All the arrangements examined in this review were initiated within the framework of the pre-2001 ministerial direction. CSIS informed the Committee that to the extent necessary, each has subsequently been modified so as to bring it into conformity with the revised direction.

The Committee's review found that the establishment of the new arrangements and the expansion of the existing ones was carried out in compliance with the

### **Policy Direction for Foreign Arrangements**

The authority to enter into arrangements with the intelligence bodies of foreign governments and international organizations is provided by the *CSIS Act*. Overall guidance is set out in ministerial direction, with specific procedures articulated in CSIS operational policy.

Ministerial direction requires that:

- arrangements are to be established as required to protect Canada's security;
- they are to be approved by the Solicitor General after consultation with the Minister of Foreign Affairs;
- the Director of CSIS shall manage existing arrangements subject to any conditions imposed by the Minister;
- the human rights record of the country or agency is to be assessed and the assessment weighed in any decision to enter into a co-operative relationship; and
- the applicable laws of Canada must be respected and the arrangement must be compatible with Canada's foreign policy.

*CSIS Act*, ministerial direction and the Solicitor General's conditions for approval. The Committee took special care to examine information relevant to the human rights records of the agencies' host countries, including open-source reporting from reputable international human rights agencies.

In this regard, the Committee took note of several new relationships where the Service will need to exercise vigilance to ensure that no information received from an agency is the product of human rights violations, and that no intelligence transferred to an agency results in such abuses. As a general rule, the Committee examines the substance of the information exchanged under any given foreign arrangement during the course of its regular reviews of individual Security Liaison Officer posts abroad.

## **B. Investigations of Complaints**

In addition to its review function, the Committee has the responsibility to investigate complaints from the public about CSIS. Where appropriate, complaints are investigated through a quasi-judicial hearing presided over by a Member of the Committee. After the hearings are complete, the presiding Member issues a report including any findings and recommendations, to both the Solicitor General and the Director of CSIS. After any information with national security implications is removed, the complainant also is advised in writing of the findings.

Through its investigations of complaints, the Committee assures itself that the Service's activities have been carried out in accordance with the *CSIS Act*, ministerial direction and CSIS policy. If we find that the Service has acted appropriately, we convey that assurance to the complainant. If the Committee identifies issues of concern, we include these in our report to the Director of CSIS and the Solicitor General and, to the extent possible, report on these matters in our annual report.

Presented below are summaries of reports on investigations issued by the Committee during the past year. Not included here are complaints that were either misdirected, or handled through administrative review or deemed to be outside the Committee's jurisdiction (*see* Table 1). The summaries are edited to protect the privacy of complainants and to prevent disclosure of classified information.

Four kinds of complaints may be directed to the Committee's attention for investigation:

- complaints lodged by persons “with respect to any act or thing done by the Service”;
- complaints received concerning denials of security clearances to government employees and contractors;
- referrals from the Canadian Human Rights Commission of complaints made to it; and
- Minister's reports in respect of the *Citizenship Act*.

## Reports of Decisions—Case Histories

The Committee reported decisions on five complaint cases during the period under review: four were complaints lodged in accordance with section 41—“any act or thing”—and one was a complaint under section 42 respecting a denial of security clearance. There were no reports on complaints referred from the Canadian Human Rights Commission or on Minister's reports.

### SECTION 41—“ANY ACT OR THING”

#### Case #1: Allegations of Undue Delay in Conducting a Security Screening Investigation

The complaint centred on two allegations. First, that the time (32 months) required by the Service to complete a security screening investigation of the complainant's application for permanent residency in Canada was unreasonable. In support of this allegation, the complainant produced documentation obtained from Citizenship and Immigration Canada (CIC) that incorrectly described the Service's role in the process. Second, that statements made by the complainant during a security screening interview with CSIS employees were not correctly reported to officials at CIC who were responsible for deciding on the application.

Based on the evidence gathered during its investigation, the Committee concluded that certain administrative elements in the conduct of the Service's investigation were unsatisfactory and did in fact contribute to an unreasonable delay. It was the Committee's opinion that the accuracy of the Service's reporting to CIC

**Table 1**  
**Resolution of Complaints\***

Description	2000–2001	2001–2002	2002–2003
Carried over	24	41	17
New	52	45	48
<b>Total</b>	76	86	65
Closed	35	69	48
Carried forward	41	17	17

\*Table 1 reflects all complaints received by the Committee. However, not all complaints received require further inquiries by the Committee nor does every complaint result in an investigation. Some are addressed by administrative action, whereas others are redirected to appropriate governmental bodies or are determined at the outset to be outside the Committee's jurisdiction.

about its interview with the complainant could be cast into doubt due to the absence of a tape-recorded interview. Finally, the Committee agreed that the CIC documentation had misinformed the complainant as to the Service's role in the immigration screening process.

Four recommendations were made by the Committee with the aim of addressing these issues. Three are classified for reasons of privacy or national security. In one recommendation, the Committee reiterated advice offered to the Service on two previous occasions, namely, that CSIS record all immigration security screening interviews and that the recordings be retained until the applicant's immigration status has been finally determined.

### **Case #2: Allegations of Unreasonable Delay in a Security Screening Investigation**

The complainant believed that the length of time required by the Service to complete its security screening investigation connected with an application for permanent residency was unreasonable. The complainant asserted that CSIS was lax in its duties and had failed to communicate adequately with either CIC or the complainant in the matter of the investigation. After reviewing the available evidence, the Committee concluded that the Service had acted appropriately and that the allegations were unfounded. The Committee made one recommendation to the Service relating to the need for certain improvements in the efficiency of handling immigration security screening requests. In response, the Service indicated that it had begun implementing these improvements by the time the report was completed.

### **Case #3: Allegations that CSIS Provided Adverse and Inaccurate Information to Foreign Authorities**

The complainant asserted that CSIS had provided adverse and inaccurate information to the authorities of a foreign country, thus causing the complainant to be briefly detained by those authorities. The complainant further asserted that the transmission of information was not a reasonable exercise of the Service's authority. Upon considering the evidence reviewed during its investigation and presented orally, the Committee concluded that the Service had acted appropriately and within the authorities granted to it by the *CSIS Act*.

### **Case #4: Allegations that CSIS Failed to Investigate Threats to the Security of Canada**

This complaint contained seven main allegations, all turning on the assertion that CSIS had failed in its duty to investigate threats to the security of Canada and advise the Government on those threats. The Committee conducted a preliminary review of the complaint and of the documentation provided by the complainant. The Committee found that three allegations related to matters best addressed by law enforcement authorities; two others concerned administrative decisions largely under the purview of federal agencies that are not within SIRC's mandate;

## **Complaints About CSIS Activities Under Section 41**

Under the provisions of section 41 of the *CSIS Act*, the Review Committee must investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before the Committee investigates, two conditions must be met:

- 1) The complainant must first have complained to the Director of CSIS and not received a response within a reasonable period of time (about 30 days) or the complainant must be dissatisfied with the Director's response.
- 2) The Committee must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith. Under section 41(2) of the Act, the Committee cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Staff Relations Act*.

and the last two raised issues already examined and reported on by the Committee in earlier reports. In view of these findings, the Committee dismissed the complaint in its entirety under section 41(1)(b) of the *CSIS Act*, which directs the Committee to investigate only if it is “satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.”

## SECTION 42—DENIAL OF SECURITY CLEARANCE

### Case #1: Revocation of a Security Clearance

The complainant was a Federal Government employee whose security clearance was revoked. As a consequence, the complainant’s employment was terminated. The complainant contested the revocation of the security clearance via an appeal to the Committee under section 42 of the *CSIS Act*. On the basis of a review of relevant documentation and after hearing witnesses’ testimony, the Committee concluded that the decision of the federal agency in question to revoke the security clearance was well founded. As required by *Government Security Policy*, the agency demonstrated that it had reasonable grounds to doubt the loyalty and reliability of the complainant. The Committee recommended that the decision of the responsible Deputy Head to revoke the clearance be upheld.

### Complaints About CSIS Activities Under Section 42

With respect to decisions to deny security clearances, section 42 of the *CSIS Act* sets out three situations in which a complaint can be made to the Committee:

- 1) any person refused federal employment because a security clearance has been denied;
- 2) any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion, for the same reason; and
- 3) anyone refused a contract to supply goods and services to the Government for the same reason.

A complaint under section 42 of the Act must be filed within 30 days of the denial of the security clearance. The Committee can extend this period if valid reasons are presented.

*For more information on how to make a complaint to SIRC, please visit our website at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)*

### **C. Section 54 Report to the Solicitor General Respecting Allegations of CSIS Misconduct**

Under section 54 of the *CSIS Act*, the Review Committee may “on request by the Minister or at any other time” forward to the Solicitor General of Canada a special report on any matter that relates to “the performance of its duties and functions.” This mechanism is employed infrequently; seven section 54 reports have been issued in the last 10 years. In 2002–2003, the Committee issued one such report to the Minister.

The report addressed alleged incidents involving the Service, which were originally brought to the attention of the Committee during the examination of a section 41 complaint. The allegations were sufficiently serious that the Committee elected to investigate the matter further. After completing our review of all relevant materials and hearing oral evidence, the Committee concluded that the original allegations were without foundation. Furthermore, the Committee saw evidence that the individual making the allegations had acted inappropriately. The Committee made several recommendations to the Service with respect to certain internal administrative and information management procedures.

## **Section 2**

---

### **CSIS Accountability Mechanisms**





## CSIS Accountability Mechanisms

### A. Policy and Governance Framework

#### **2002–2003 NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE**

National Requirements contain general direction from government as to where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities. Because the 2001–2002 National Requirements were issued before the events of September 11, 2001, this year's requirements document is the first to address directly the post-September 11 environment.

Overall, the 2002–2003 requirements reflect the impact that new pressures and heightened public awareness have had on intelligence priorities. Although the 2002–2003 requirements are generally consistent with the direction given in previous years, several items drew the Committee's attention:

- CSIS was directed to co-operate with other departments of government so as to facilitate the prosecution or deportation of key members of terrorist organizations and to deny terrorist organizations a safe haven in Canada.
- Measures to counter the proliferation of weapons of mass destruction were identified as a more urgent priority since September 11, 2001.
- Considerable attention is given in the 2002–2003 National Requirements to the Service's role in security screening, especially in relation to preventing persons of security concern from entering the country.
- The Service was directed to upgrade, expand or replace technical equipment and information systems, as required, to ensure national security.

#### **MINISTERIAL DIRECTION**

Under section 6(2) of the *CSIS Act*, the Minister can issue directions governing CSIS's activities and investigations. No new directions were issued in the year under review.

#### **GOVERNOR IN COUNCIL REGULATIONS AND APPOINTMENTS**

As set out in section 8(4) of the *CSIS Act*, the Governor in Council may issue any regulations to the Service in regard to the powers and duties of the Director

of CSIS, as well as the conduct and discipline of Service employees. No such regulations were issued during 2002–2003.

### **SECTION 28 REGULATIONS**

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies to the Federal Court for warrants. In 2002–2003, no such regulations were issued.

### **CHANGES IN CSIS OPERATIONAL POLICY**

Together with the *CSIS Act* and ministerial direction, CSIS operational policy provides parameters and guidelines for the Service's activities and investigations. The Committee examined 8 new operational policies issued by the Service in 2002–2003 and 44 amendments to existing CSIS policies.

Although there were twice as many new policies this year than last, the most recent additions related essentially to two key areas of Service operations: co-operating with domestic government departments and agencies, and reporting operational information. One new policy provided direction on the Service's disclosure of national security-related information to Canada Customs and Revenue Agency for enforcement purposes. A second policy set out procedures for Service support to CIC in the screening of refugee claimants and foreign nationals.

Six other new policies set out the parameters and procedures for reporting, recording and tracking operational information collected by the Service for use by its employees in conducting investigations.

With respect to the 44 amended policies, almost half were the result of the Counter Intelligence and Counter Terrorism branches being reorganized to create a third branch, Counter Proliferation (*see* CP branch description page 35). Three revisions were made to reflect changes in Government Security Policy and two others related to the handling of human sources.

Thirteen updates were made to certain procedures and powers in the conduct of investigations and the balance reflected changes necessary to bring policies into conformity with the March 2001 compendium of ministerial direction.

Because of national security concerns, the Committee is unable to elaborate further on these additions to Service policy. We have examined them in detail, however, and we are satisfied that both the new and revised policies conform to the *CSIS Act* and ministerial direction.

## B. Reporting Requirements

### **CERTIFICATE OF THE INSPECTOR GENERAL FOR 2002**

The Inspector General of CSIS reports to the Solicitor General and functions in effect as the Minister's internal auditor of CSIS, reviewing the operational activities of the Service and monitoring compliance with policy and the *CSIS Act*. Each year, the Inspector General (IG) must submit to the Minister a certificate stating the "extent to which [he or she] is satisfied" with the Director's Annual Report to the Solicitor General on the operational activities of the Service, and informing the Minister of any instances of CSIS failing to comply with the Act or ministerial direction, or which involved an unreasonable or unnecessary exercise of powers. As per section 33(3) of the Act, the Minister forwards the certificate to SIRC for its consideration.

In reviewing the Inspector General's certificate, SIRC noted that the IG followed a methodology consistent with the previous year. His review consisted of the inspection of documentation supporting the Director's report to the Minister, an analysis of significant Service operations, and interviews with senior CSIS management at HQ and in the field. He based his conclusions on a validation process that included an inspection of CSIS internal documents and a review of the "facing" documentation, supplemented by the IG's annual program of review activities, which this year included *inter alia* a review of samples of warrants and targets and a detailed examination of certain CSIS investigations.

In this year's certificate, the Inspector General stated that over the 18 years since CSIS was created the "Service has demonstrated a steadily improving organizational maturity and professionalism as a security intelligence service." With respect to the Director's Annual Report for 2001–2002, he declared himself to be "fully satisfied." It was his opinion that the Service had not acted beyond the framework of its statutory authority, contravened any ministerial direction or exercised its power unreasonably or unnecessarily.

The Inspector General also commented on CSIS's response to the events of September 11, 2001 and Sunni Islamic extremism. He felt that the Service had positioned itself well to respond to the Sunni Islamic threat and showed considerable flexibility and skill in reallocating resources to address the new, unprecedented threat environment. In his view, the response to the terrorist attacks was measured, properly situated within the Service's statutory framework and very effective. He attributed this in significant measure to the Service's excellent relationships with police forces in major urban centres across the country.

### **CSIS ANNUAL OPERATIONAL REPORT FOR 2001–2002**

In accordance with section 33(1) of the *CSIS Act*, the Director of CSIS is required to submit an annual report to the Solicitor General detailing the operational activities of the Service. Further, under section 33(3) of the Act, the Minister must provide SIRC with a copy of the Director's report, which, pursuant to section 38, SIRC is then required to review.

The Director's report describes the investigations and operational activities of the Service and identifies significant achievements or challenges in its operations. This year represents the Committee's second opportunity to review the abbreviated reporting structure recommended by the Inspector General of CSIS and adopted by the Service in November 2000. Additional detail in support of the report to the Minister is made available in extensive supplementary documentation.

The report outlines the Service investigations conducted during the fiscal year 2001–2002, including individual reporting on each of the Service's branches. It also covers the first full year of operational activity under the new compendium of ministerial direction, effective March 1, 2001, and commented on by SIRC in its 2000–2001 Annual Report. The additional program and activity details provided in this year's report are an improvement over last year's document, and yearly comparisons of CSIS activities and descriptions of new programs will allow the Committee to select topics for future research and be aware of growing pressures on CSIS to meet its obligations.

The Director's 2001–2002 report speaks to specific challenges arising from international events and identifies the CSIS operational activities and programs that are beginning to gain from the new funds approved in the December 2001 federal budget. The Committee will continue to closely monitor both areas.

### **UNLAWFUL CONDUCT**

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

In 2002–2003, the Service sent no reports of illegal activity to the Minister. An instance of unlawful conduct originally reported in the Committee's 2000–2001 Annual Report is still being considered by the Attorney General of Canada.

### **SECTION 2(D) INVESTIGATIONS**

According to ministerial direction, any investigation of threats to the security of Canada as defined in section 2(d) of the *CSIS Act*—often referred to as the

“subversion” clause—must be authorized by the Minister. The Service reported that the Minister authorized no such investigations in 2002–2003.

### **DISCLOSURES OF INFORMATION IN THE PUBLIC OR NATIONAL INTEREST**

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigations from being disclosed except in specific circumstances. Under Section 19(2)(d) the Minister can authorize the Service to disclose information in the “public interest.” The Service reported no such disclosures in 2002–2003.

In addition, CSIS, acting as the Minister’s agent, can disclose information in the “national interest” under specified circumstances. The Service reported that there were no such disclosures during the year under review.

## **C. CSIS Operational Activities**

In addition to carrying out in-depth reviews of selected CSIS operations each year, the Committee requests written and oral briefings from the Service about several activities that are relevant to the Committee’s mandate. The information we receive relates to the Service’s plans and priorities, especially as they pertain to its main operational branches. Although this information is not independently verified unless it forms part of an in-depth Committee review, it nonetheless helps the Committee to stay apprised of and to monitor the Service’s priorities and perspectives, from year to year.

This section of the Annual Report summarizes information the Committee received in written and oral briefings. It also provides data obtained from the Service in accordance with section 38(a)(vii) of the *CSIS Act*, which requires the Committee to compile and analyze statistics on the operational activities of the Service.

### **COUNTER PROLIFERATION**

In a significant restructuring of its operational programs, CSIS created in July 2002 a new branch devoted to countering the proliferation of weapons of mass destruction. The goals of the Counter Proliferation (CP) branch, the Service reported, are to identify countries developing nuclear, chemical or biological weapons and gather information about these activities so as to advise the Government on possible threats to Canada’s national security and public safety.

Among CP's most important concerns is the potential threat posed by terrorist organizations that might manage to obtain the information and materials necessary to use such weapons themselves. According to the Service, the CP branch integrates programs, personnel and resources previously located in the Counter Terrorism and Counter Intelligence branches. The reorganization is intended to better focus existing technical skills and investigative resources.

Given that CSIS is refocusing its operations to counteract the proliferation of weapons of mass destruction and in light of the importance that CSIS has given to this organizational restructuring, the Committee sought and received a detailed classified briefing from the Service about its scope and intent. Our in-depth reviews will encompass this new operational branch and we will report our findings in future annual reports.

### **COUNTER TERRORISM**

The role of the Counter Terrorism (CT) branch is to advise the Government on emerging threats of serious violence that could affect the safety and security of Canadians and of Canada's allies. Whether of domestic or foreign origin, addressing the threat of violence in support of political, religious or ideological objectives continues to be one of the Service's chief priorities.

The Service reported a significant reorganization of CT branch's structure in 2002–2003. Several operational units were transferred to the newly created Counter Proliferation branch. Other areas were restructured to improve effectiveness and to handle added responsibilities arising out of new and revised legislation—most notably the *Anti-terrorism Act*.

As in 2001–2002, the threats presented by Sunni Islamic terrorism remained a major focus of CT's operational activities. According to the Service, the interdiction and removal of suspected terrorists continued to be a key objective. Investigations aimed at preventing terrorists from using Canada as a venue for financing operations have also grown in importance and complexity.

In this Annual Report, the Committee has examined Service investigations of Sunni Islamic extremism as viewed through two studies. Future Annual Reports will present results of other reviews of counter-terrorism investigations carried out by the Service.

### **Threat Assessments**

CSIS provides threat assessments to departments and agencies within the Federal Government based on relevant and timely intelligence. CSIS prepares these

assessments—dealing with special events, threats to diplomatic establishments in Canada and other situations—either upon request or unsolicited.

The CSIS unit responsible for preparing threat assessments was moved from CT branch to the newly created CP branch part way through the period under review. Between them, CT and CP branches issued 659 threat assessments in 2002–2003. This number was smaller than the year previous but still an increase over 2000–2001.

As in the past, the Committee continues to examine those threat assessments that are relevant to its in-depth reviews of CSIS operational activities.

### **COUNTER INTELLIGENCE**

The Counter Intelligence (CI) branch investigates threats to national security caused by the hostile intelligence activities of foreign governments, as well as threats to Canada's social, political and economic infrastructure. The Service reported that since the threat environment had altered little since the previous year, the operational and investigative focus of the CI program remained essentially unchanged.

There was some organizational restructuring to reflect changes brought about by the new *Security of Information Act* and to foster greater administrative streamlining generally. In addition, CI's program on the proliferation of weapons of mass destruction was made part of the new CP branch.

As in previous years, the Service's counter intelligence activities continue to form part of the Committee's review of Service operations.

### **RESEARCH, ANALYSIS AND PRODUCTION**

The Service's Research, Analysis and Production (RAP) branch is responsible for producing and disseminating finished intelligence product to the Government of Canada on threats to the security of Canada through such documents as CSIS Reports, CSIS Studies and CSIS Intelligence Briefs. When appropriate, RAP intelligence product is also distributed to a broader readership.

Authorized disclosures of information obtained in the performance of CSIS's duties and functions—subject to section 19(2)(a) through (d) of the *CSIS Act*—are another means by which RAP disseminates intelligence product. RAP reported that in 2002–2003 there were 1335 section 19 disclosure reports, an increase over the 778 reports in 2001–2002.

In 2002–2003, RAP also produced 61 classified reports compared to 83 the previous year. RAP's intelligence publications generally fall under two categories:



- Public safety reports examine the threat to Canadians at home and abroad from international terrorism.
- National security reports address activities in Canada of other governments' intelligence services, as well as global issues such as counter proliferation and transnational criminal activity.

Through RAP, CSIS also contributes to the wider government intelligence community by participating in the Intelligence Assessment Committee (IAC). This body is made up of senior officials from departments and agencies of the Government of Canada most concerned with intelligence matters. In the year under review, RAP staff wrote or contributed to the writing of 13 IAC reports.

The Committee uses RAP reports, studies and briefs to obtain context for the Service's investigations, to identify the Service's perspective on specific threats, and to enhance its own knowledge of the nature of the analysis and advice, which CSIS provides to government pursuant to section 12 of the *CSIS Act*.

### **SECURITY SCREENING**

The Service has the authority, under section 13(1) of the *CSIS Act*, to provide security assessments to federal government departments. The Service may also, with appropriate Ministerial approval, enter into arrangements to provide assessments to provincial government departments or provincial police forces, as outlined in section 13(2). Arrangements for providing security screening advice to foreign governments, foreign agencies and international institutions and organizations are authorized under section 13(3).

For federal employment, CSIS security assessments serve as the basis for determining whether an individual should be granted access to classified information or assets. In immigration cases, Service assessments can be instrumental in CIC's decision to admit an individual into the country and in granting either permanent resident status or citizenship.

CSIS reported to the Committee that it had significantly expanded its security screening program—performed on a cost-recovery basis—for non-federal agencies. These new clients include several provincial governments and operators of nuclear power facilities. CSIS also reported that an increasing proportion of its security screening cases were being processed electronically, permitting greater efficiency in the delivery of security screening services to a growing list of clients.

Another event that impacted the Branch in 2002–2003 was the coming into force in June 2002 of the new *Immigration and Refugee Protection Act*, which

## Nature of CSIS Advice to CIC

The Service's security screening assessments are provided as advice to CIC in one of four forms:

**No Reportable Trace (NRT)**—a report given to CIC when the Service has no adverse information on the immigration applicant.

**Inadmissible Brief**—advice provided when the Service has concluded, based on information available to it, that the applicant meets the criteria outlined in the security provisions of the *Immigration and Refugee Protection Act*.

**Information Brief**—advice provided by CSIS that it has information that the applicant is or was involved in activities as described in the security provisions of the *Immigration and Refugee Protection Act*, but that it is of the opinion that the applicant does not fall into the class of persons deemed to be inadmissible under the Act.

**Incidental Letter**—provided to CIC when the Service has information that the applicant is or was involved in non-security-related activities described in the *Immigration and Refugee Protection Act* (for example, war crimes or organized criminal activity) or any other matter of relevance to the performance of duty by the Minister of Citizenship and Immigration, as set out in section 14(b) of the *CSIS Act*.

superceded the *Immigration Act*. The new Act governs the policies and operations of CIC, the Service's largest security screening client.

### Immigration Security Screening Programs

Under the authority of sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to the Minister of Citizenship and Immigration Canada (CIC). Generally speaking, the Service's assistance takes the form of information-sharing on matters concerning threats to the security of Canada as defined in section 2 of the *CSIS Act* and the form of "assessments" with respect to the inadmissibility classes of the *Immigration and Refugee Protection Act*.

Immigration requests for security screening resulted in 445 briefs from CSIS to CIC—242 information briefs and 203 inadmissible briefs. Of those requests, the median time required for a "no reportable trace" (NRT) was 57 days, for an information brief 400 days and for an inadmissible brief 461 days. For the year previous, the median figures were 55 days, 401 days and 498 days, respectively.

Unlike previous years, the Service reported on citizenship applications as a separate category. An information brief with respect to a citizenship application took a median time of 129 days.

During fiscal year 2002–2003, the Service provided 87 update letters (updates to briefs) and 22 incidental letters to CIC.

#### **Applications for Permanent Residence from Within Canada**

The Service has the sole responsibility for screening immigrants and refugees who apply for permanent residence status from within Canada. In 2002–2003 the Service received 33 837 such screening requests. Of these requests, 21 950 were immigration applications and 11 887 came through the Refugee Determination Program.

According to the statistical information provided by the Service, the time required for the Service to issue a recommendation on an immigration application varies considerably depending on how the application was filed. Those applications filed using the Electronic Data Exchange from within Canada took a median of 45 days, and electronic filings within the Refugee Determination Program took 55 days. For those applications filed on paper, the median turnaround time for immigration applications from within Canada was 70 days; for applications from the U.S. it was 150 days, and for paper applications from within the Refugee Determination program 94 days.

#### **Application for Permanent Residence from Outside Canada**

Immigration and refugee applications for permanent residence that originate outside Canada or the United States are managed by the Overseas Immigrant Screening Program under which the Service shares responsibility for security screening with CIC officials based abroad. Generally, CSIS only becomes involved in the screening process either upon being requested to do so by the Immigration Program Manager or upon receiving adverse information about a case from established sources. CSIS reports that this division of labour allows the Service to concentrate on higher-risk cases.

In 2002–2003, the Service received 23 691 requests to screen refugee and immigration applications initiated outside Canada. Of these, CSIS reported that 6776 were referred to Security Liaison Officers (SLOs) for consultation, marginally fewer than the year previous.

#### **Citizenship Applications and the Watch List**

As part of the citizenship application process, the Service receives electronic trace requests from CIC's Case Processing Centre in Sydney, N.S. The names of the

citizenship applicants are cross-checked against the names in the Security Screening Information System database. The Service maintains a Watch List that contains the names of individuals who have come to the attention of CSIS through, *inter alia*, Target Approval and Review Committee–approved investigations.

In 2002–2003, the Service reviewed 158 675 citizenship applications for CIC. Of these, 185 resulted in information briefs. The Service reported issuing no inadmissible briefs. In six instances CSIS reported seeking Ministerial approval to defer its advice.

### **Front-End Screening**

The Front-End Screening (FES) program was implemented by the Government to identify and filter potential security and criminal cases from the refugee claimant stream as early as possible in the determination process. For fiscal year 2002–2003—the first full year in which the program was active—the Service reported receiving 27 407 cases from CIC for processing. Of these, 21 735 were completed by March 31, 2003.

CSIS advised the Committee that administrative difficulties in the transfer of information from CIC that created delays at the startup of the program had since been rectified. The Committee is reviewing the Service’s participation in the FES program and will report its findings in a future annual report.

### **Screening on Behalf of Foreign Agencies**

The Service may enter into reciprocal arrangements with foreign agencies to provide security checks on Canadians and other individuals who have resided in Canada. For 2002–2003, the Service reported that 1797 screening checks were carried out on behalf of foreign agencies. Of these, 177 resulted in field investigations.

In a clarification of information provided previously to the Committee and presented in last year’s Annual Report, the Service advised the Committee that it does not make recommendations to foreign agencies to deny security clearances. The Service only provides the results of findings, either as a NRT report or a report of adverse information in the form of an information brief.

### **Security Screening for Federal Employees**

#### 2002–2003 Key Statistics

- The Service received 51 262 requests for security screening assessments for clearance, levels one through three, new, upgraded and updated. Also, 870 requests were for action relating to administrative procedures such as downgrades and transfers.

- The Committee asked CSIS to report the median turnaround time for security assessments in two separate categories—Department of National Defence (DND), and all other government departments and agencies. For the period 2002–2003, the Committee noted that the turnaround time for DND assessments, as compared with other government departments, has been considerably reduced from the previous year (Table 2).
- The Service informed us that it conducted 3578 field investigations in order to complete the security screening requests from all government departments and agencies.
- The Service received 34 010 requests for assessments under the Airport Restricted Access Area Clearance Program (ARAACP). This number represents a marginal increase over the previous fiscal year. At 15 days, the median turn around time for ARAACP requests was unchanged from the previous year.
- There were 13 613 requests for security assessments related to “site access,” with requests coming primarily from Ontario Power Generation, Bruce Power, Atomic Energy of Canada and the National Capital Commission.
- The Service reported that their security screening investigations resulted in 26 information briefs and 3 denial briefs.
- CSIS processes certain categories of security screening site access requests with the RCMP acting as intermediary on behalf of the original requester. In 2002–2003, the Security Accreditation Program processed approximately

**Table 2**  
**Turnaround Times for Security Screening**

Category	Level	Median Number of Days	Median Number of Days
		2001–2002	2002–2003
DND	1 (Confidential)	43	28
	2 (Secret)	50	29
	3 (Top Secret)	97	47
Government	1 (Confidential)	2	5
	2 (Secret)	30	13
	3 (Top Secret)	62	51

1450 requests for the Parliamentary Precinct (which includes all facilities, offices and buildings controlled by the Parliament of Canada) and some 13 500 requests for accreditation to other special events and functions to which access is controlled.

- The Service reported that more than 82 percent of screening requests from government clients were processed through the EDE program. The Service also informed the Committee about already implemented and proposed expansions of the EDE program in its SLO posts abroad.

## **CSIS DOMESTIC AND INTERNATIONAL ARRANGEMENTS**

### **Relations with the RCMP**

Among the Service's domestic liaison partners, the Committee has always paid particular attention to CSIS's arrangements with the RCMP. Again this year, the Service reported that its relationship with the RCMP was undergoing considerable change—a process driven by the increased awareness by government of the need to protect public safety and national security, and by significant new legislation enacted since the events of September 11, 2001.

For the year under review, the Service recorded 2270 written exchanges (originating from either direction) with the RCMP, compared to 1503 in 2001–2002. The Service sent 221 disclosure letters to the RCMP (of which 91 related to the Air India disaster) and 6 advisory letters.

The Service noted that the most important change in its operational liaison with the RCMP was in the manner in which the two organizations exchange personnel. Following a 2001–2002 pilot program carried out in a particular region allowing for mutual secondments of officers, the Service reported that similar arrangements had been fully implemented in three regions of the country. Structured around the RCMP's INSET (Integrated National Security Enforcement Teams) program, the goal of the secondment arrangements is to foster closer operational co-operation between CSIS and the RCMP so that “each party can better respond to common requirements in the area of national security.”

The Service reported that although it was generally pleased with how these new regionally based coordinating bodies had developed, working arrangements and protocols were still being refined. In the Service's view, the INSET program was not sufficiently far along in its implementation to measure successes or identify

particular concerns. The Service's participation in the INSET program will be part of a future Committee review of the Service's domestic co-operative relationships.

The Service also reported that, besides on-going exchanges of personnel, CSIS officers contributed to several RCMP training programs and for the first time participated in a key RCMP operational planning session.

Of major importance for the CSIS–RCMP relationship, from the Service's point of view, was the *Anti-terrorism Act* enacted in late in 2001. Criminalizing a range of activities specifically related to terrorism put an added premium on closer co-operation between law enforcement and intelligence agencies and, according to CSIS, was directly responsible for the increase in flow of operational exchanges between the two organizations.

#### **Other Domestic Arrangements**

In carrying out its mandate CSIS co-operates both with police forces and with federal and provincial departments and agencies across Canada. Contingent on Ministerial approval, the Service may conclude written co-operation arrangements with domestic agencies pursuant to section 17(1) of the *CSIS Act*.

In the year under review, the Service finalized one new letter of agreement, in this case with a provincial body.

#### **Foreign Arrangements**

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

The Service reported that during fiscal year 2002–2003 it had received the Minister's approval to establish 5 new liaison arrangements and to modify arrangements with 21 others. The Service continued to maintain restrictions on exchanges of information with five agencies due to concerns either about the agencies' human rights records, violations of the rule against transferring information to third parties or their overall reliability.

The Service also reported that of the 237 established foreign arrangements, 42 were regarded as dormant (dormancy is defined as no liaison contact for at least

one year). Requests for 7 proposed new arrangements have been submitted by CSIS to the Solicitor General and are still under consideration. The Committee continues to monitor the Service's foreign arrangements and will convey our findings in a future annual report.

As part of its foreign liaison program, the Service maintains liaison posts abroad normally co-located with Canadian diplomatic missions. CSIS opened three new posts during 2002–2003 and is expected to open another during fiscal year 2003–2004. The Service reported that the most significant challenge to the foreign liaison program, as in recent past years, was that its overseas posts continue to face an ever-increasing security screening workload arising from its program of assistance to CIC. As in previous years, the Committee will conduct a review of a specific liaison post and report its findings in due course.

### FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone their use bears continued scrutiny—a task that the Committee takes very seriously. In the course of our in-depth reviews of CSIS investigations, warrants are generally the subject of detailed examination. In the past, the Committee has also focused solely on warrants as an individual study.

Each year, the Committee asks CSIS to provide statistics about CSIS warrant applications and on warrant powers granted by the Federal Court. Table 3 compares the number of warrant powers issued in each of the last three fiscal years.

According to the Service, the Federal Court issued 25 urgent warrant powers during 2002–2003 compared to 49 in the previous year. Although no applications for warrants were denied by the Court, CSIS reported six instances where the presiding Federal Court Judge requested significant amendments prior to issuing the warrant.

**Table 3**  
**New and Replaced/Renewed Warrant Powers**

	2000–2001	2001–2002	2002–2003
New warrant powers	56	111	52
Replaced/renewed warrant powers	150	155	150
Total	206	266	202



Two new conditions were imposed by the Court, both to be included in all future warrants where relevant. One condition related to obtaining financial records, whereas the second pertained to how persons subject to warrant powers are identified. As a general rule, conditions in a warrant serve to restrict how CSIS may exercise its warrant powers or what it may do with the information collected during its execution.

Finally, CSIS implemented four revisions to existing warrant powers—two were case specific, whereas the other two have become standard in all future warrants. Among the latter, one ensured consistency with new legislation and the other expanded the legal definition of a certain technical device.

The Service reported that in 2002–2003 there were no judicial decisions with significant impact on any individual warrant power or on the warrant process generally.

#### **Warrant Statistics in Perspective**

Although the data collected by the Committee provide insight into how often the Service seeks warrant powers from the Federal Court in a given year, comparing these numbers between years is of limited use. A range of factors, as disparate as court decisions and new developments in technology, introduce significant variations into how often warrant powers are applied for and how they are implemented. In addition, a single warrant can authorize the use of several warrant powers against one person, several people or an organization. Considered in isolation, therefore, warrant numbers are not a definitive indicator of the level of Service investigative activity. It is also important to bear in mind that warrants are only one of several investigative instruments available to CSIS.

## **Section 3**

---

### **Inside the Security Intelligence Review Committee**



## Inside the Security Intelligence Review Committee

### **APPOINTMENT OF A NEW MEMBER**

In February 2003, the Governor in Council appointed the Honourable Baljit S. Chadha as a Member of the Committee for a five-year term. Mr. Chadha is the President of Montreal-based Balcorp Limited and a member of the Board of Governors of Concordia University.

### **SENIOR STAFF APPOINTMENTS AT SIRC**

In October 2002, Susan Pollak, Executive Director of SIRC, announced the appointment of Kelly McGee as the Deputy Executive Director. Most recently, Ms. McGee was the Research Manager for SIRC following many years as Senior Counsel and Director of Policy and Legislative Services at the Regional Municipality of Ottawa–Carleton.

In March 2003, Suzanne Beaubien joined SIRC as Research Manager. Previously, Ms. Beaubien was the Senior Policy Analyst in the Public Health Branch of the Ontario Ministry of Health and Long-Term Care, with 21 years' experience in communications and program analysis within the Ontario public service. A seasoned journalist, she was the Queen's Park correspondent for the CKO All News national network.

### **SIRC STAFFING AND ORGANIZATION**

As of March 31, 2003 the Committee had a staff complement of 16: an Executive Director, a Deputy Executive Director, a Senior Counsel, a Counsel, a Senior Paralegal and an Access to Information and Privacy Officer/Analyst (both of whom are Committee registrars for hearings), a Research Manager, two Senior Research Advisors, one Senior Research Analyst, two Research Analysts, a Financial/Office Manager, and an administrative support staff of three to handle sensitive and highly classified material using special security procedures.

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

**RESEARCH AND REVIEW ACTIVITIES**

Each fiscal year the Committee identifies a number of areas of CSIS activity that will be the focus of its review. Reporting regularly to senior management and to Committee Members at their meetings, SIRC researchers and analysts divide their time between SIRC's premises and the Committee's facilities at the Service. The separate office space and computers made available by the Service at CSIS Headquarters are for the exclusive use of SIRC staff.

**SECURITY INTELLIGENCE BRIEFINGS**

As part of their regular meetings the Chair and Committee Members have exchanges with senior government officials within Canada's security intelligence community, academics and other experts in the field, or with key non-governmental organizations in order to keep lines of communication open and to stay abreast of new developments. Committee meetings are frequently held in different regions of the country, at which time Members also visit CSIS regional offices to be briefed on local operational priorities and challenges.

**PARLIAMENTARY RELATIONS**

On February 18, 2003, Committee Chair Paule Gauthier and Members Gary Filmon and Raymond Speaker appeared before the House of Commons Subcommittee on National Security. Also present were SIRC's Executive Director, Deputy Executive Director and Senior Counsel.

**ADDITIONAL COMMITTEE ACTIVITIES**

In May 2002, the Committee Chair Paule Gauthier, Member Raymond Speaker and the Executive Director attended a gathering of international intelligence review agencies in London, England.

In June 2002, research staff attended the Canadian Centre of Intelligence and Security Studies' (CCISS) inaugural conference held at Carleton University, Ottawa. The theme of the Conference was "Canada's Foreign Intelligence Requirements: Threats, Capabilities and Options." In July 2002, Susan Pollak, SIRC Executive Director, accepted an invitation to join CCISS's Council of Advisors.

In September 2002, the Executive Director and staff attended the conference of the Canadian Association of Security and Intelligence Studies held in Ottawa. The conference theme was: "The New Intelligence Order: Knowledge for Security and International Relations."

In October 2002, SIRC's Executive Director addressed a graduate seminar at the Centre for Security and Defence Studies, The Norman Paterson School of International Affairs, Carleton University, in Ottawa.

In February 2003, SIRC senior management and research staff attended the conference of the Law Commission of Canada with the theme "In Search of Security: An International Conference on Policing and Security" held in Montreal.

In March 2003, senior management and staff attended the 2003 CCISS conference in Ottawa entitled: "Intelligence Analysis: Recent Trends, Canadian Requirements." SIRC's Executive Director participated in the conference's summing up round table.

### **BUDGET AND EXPENDITURES**

The Committee continues to manage its activities within allotted resource levels. The chief expenses were for staff salaries and benefits and for travel expenses within Canada for Committee hearings, briefings and review activities (Table 4).

### **SIRC REQUEST FOR INCREASED FUNDING**

In the Committee's annual report of 2001–2002 we reported on the substantial new resources the Government had allocated to CSIS, namely, an immediate increase in budget of 30 percent. We noted that as a direct and immediate result of this increase, the Service was dramatically raising the level of investigative activities that SIRC has a legal responsibility to monitor and review.

SIRC then undertook a comprehensive review of its own activities and the resources available to fulfill its obligations to Parliament and the people of Canada. As a result, in July 2002 the Committee made a formal request to Treasury Board for an increase in resources of 16 percent. If granted, this would

**Table 4**  
**SIRC Expenditures**

	<b>2002–2003</b> (Actual \$)	<b>2003–2004</b> (\$ Estimates)
Personnel	1 438 344	1 363 000
Goods and Services	659 892	975 000
<b>Total</b>	<b>2 098 236</b>	<b>2 338 000</b>

provide the Committee with additional financial resources commensurate with CSIS's expanded level of activities.

#### **INQUIRIES UNDER THE ACCESS TO INFORMATION AND PRIVACY ACTS**

Every year, SIRC receives requests for the release of material under both the *Access to Information Act* and the *Privacy Act*. Table 5 records the number of requests for the past three fiscal years.

Because the Committee receives numerous requests for the same SIRC study the work required to process the first request for any given study does not have to be repeated. The Committee has chosen, therefore, to waive application fees for access to studies.

**Table 5**  
**Requests for Release of Material**

Year	<i>Access to Information Act</i>	<i>Privacy Act</i>
2000–2001	34	3
2001–2002	22	4
2002–2003	20	4

## **Appendix A**

---

### **Acronyms**





---

## Acronyms

ARAACP	Airport Restricted Area Access Clearance Program
CCISS	Canadian Centre of Intelligence and Security Studies
CCRA	Canada Customs and Revenue Agency
CI	Counter Intelligence branch
CIC	Citizenship and Immigration Canada
CP	Counter Proliferation branch
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism branch
DND	Department of National Defence
FES	Front-End Screening program
HQ	CSIS Headquarters, Ottawa
IAC	Intelligence Assessment Committee
IG	Inspector General
INSET	Integrated National Security Enforcement Team
MOU	Memorandum of Understanding
NRT	“no reportable trace”
RAP	Research, Analysis and Production branch
RCMP	Royal Canadian Mounted Police
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer



## **Appendix B**

---

### **SIRC Reports and Studies Since 1984**



## SIRC Reports and Studies Since 1984

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

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

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

28. *Report on Multiple Targeting* (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq* (SECRET) (91/92-01)
30. *Report on Al Mashat's Immigration to Canada* (SECRET) \* (91/92-02)
31. *East Bloc Investigations* (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions* (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)
34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) \* (91/92-04)
35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study* (SECRET) \* (91/92-07)
38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) \* (92/93-01)
39. "STUDYNT" *The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) \* (90/91-13)
41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) \* (90/91-10)



45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review* (TOP SECRET) \* (91/92-14)
46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)* (TOP SECRET) \* (90/91-11)
47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)
48. *Domestic Exchanges of Information (A SIRC Review—1991/92)* (SECRET) (91/92-16)
49. *Prairie Region Audit* (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)
51. *Regional Audit* (TOP SECRET)
52. *A SIRC Review of CSIS' SLO Posts (London & Paris)* (SECRET) (91/92-11)
53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)
54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93-03)
55. *Domestic Investigations (1)* (SECRET) (CT 93-02)
56. *Domestic Investigations (2)* (TOP SECRET) (CT 93-04)
57. *Middle East Movements* (SECRET) (CT 93-01)
58. *A Review of CSIS SLO Posts (1992-93)* (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93-11)

64. *Sources in Government* (TOP SECRET) (CI 93-09)
65. *Regional Audit* (TOP SECRET) (CI 93-02)
66. *The Proliferation Threat* (SECRET) (CT 93-07)
67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) \* (CT 94-02)
68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)
69. *Domestic Exchanges of Information (A SIRC Review 1993-94)* (SECRET) (CI 93-08)
70. *The Proliferation Threat—Case Examination* (SECRET) (CT 94-04)
71. *Community Interviews* (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) \* (CI 93-07)
73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS SLO Posts (1994-95)* (SECRET) (CT 95-01)
75. *Regional Audit* (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994-95)* (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
82. *CSIS and a "Walk-In"* (TOP SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)
85. *Regional Audit* (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)
88. *Homeland Conflict* (TOP SECRET) (CT 96-01)
89. *Regional Audit* (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources* (TOP SECRET) (CI 96-03)
91. *Economic Espionage I* (SECRET) (CI 96-02)
92. *Economic Espionage II* (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96-04)
94. *Urban Political Violence* (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information (1996–97)* (SECRET) (SIRC 1997-02)
96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997-03)
97. *Regional Audit* (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997-05)
99. *Spy Case* (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations (3)* (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation with the RCMP—Part I* (SECRET) \* (SIRC 1998-04)

102. *Source Review* (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998-08)
105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)
106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *CSIS Cooperation with the RCMP—Part II* (SECRET) \* (SIRC 1998-04)
109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98* (TOP SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)
113. *Allegations by a Former CSIS Employee* (TOP SECRET) \* (SIRC 1998-12)
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC 1998-15)
116. *Files* (TOP SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET) (SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET) (SIRC 1999-02)
119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) \* (SIRC 1999-05)
122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)
123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)
124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)
125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)
126. *Project Sidewinder* (TOP SECRET) (SIRC 1999-10)
127. *Security Breach* (TOP SECRET) (SIRC 1999-11)
128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)
130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)
131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)
132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)
134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET) (SIRC 2002-01)
135. *Source Recruitment* (TOP SECRET) (SIRC 2001-01)
136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001-05)
137. *Domestic Extremism* (TOP SECRET) (SIRC 2001-03)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET) (SIRC 2001-04)

139. *Warrant Review* (TOP SECRET) (SIRC 2001-06)
140. *Special Report following allegations pertaining to an individual* (TOP SECRET) \*
141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)
142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)
143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)
144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)
145. *Special Report (2002-2003) following allegations pertaining to an individual* (TOP SECRET) \*



## **Appendix C**

---

### **Key Findings and Recommendations**





## Key Findings and Recommendations

### IN THE MATTER OF AHMED RESSAM

On December 14, 1999, Ahmed Ressam was arrested while attempting to enter the United States from Canada with explosives hidden in the trunk of his rental car. Ressam was subsequently convicted on charges related to his unsuccessful attempt to carry out a terrorist attack at the Los Angeles International Airport to mark the beginning of the new millennium.

Upon reviewing all the relevant documentation, the Committee concluded that the Service did not possess specific information that would have forewarned it of Ressam's planned terrorist operations. In the Committee's view, the actions CSIS took to locate Ressam in 1999 were appropriate in light of the information available at the time. The Committee saw no evidence that it was a lack of vigilance on the part of the Service that contributed to Ressam's ability to escape detection after his return in 1999 to Canada.

The Committee found that the Service's investigative activities following Ressam's arrest were appropriate and proportionate to the threat. The Service complied with the requirements of law, ministerial direction and policy.

This case showed the capacity of the Service and the RCMP to assist each other effectively while working within their respective mandates. Similarly, the exchanges of information between the Service and its U.S. partners were timely and comprehensive, indicating a smooth-functioning and productive relationship.

### SUNNI ISLAMIC EXTREMISM—A REVIEW OF CSIS REGIONAL INVESTIGATIONS

The Committee examined all electronic and hard-copy documentation during the review period related to five broad operational activities:

- 1) the targeting request and approval process, and the investigating of targets;
- 2) the acquiring and implementing of warrants;
- 3) the recruiting, developing and directing of human sources;
- 4) the conducting of interviews in the community; and
- 5) the exchanging of information and other forms of liaison with domestic agencies.

#### Targeting and Investigations

The Committee found that in all cases the Service had reasonable grounds to suspect the target's involvement in activities that constituted a threat to the security of

Canada and that the levels of investigation were proportionate to the threat activities observed.

In obtaining targeting authorities and conducting the investigations, the Service met all the requirements set out in law, ministerial direction and operational policy. It collected only the information strictly necessary for the investigation.

Two instances drew the Committee's attention and required additional inquiries of the Service. In the first, the Committee reviewed documentation about an unusual event involving one of the selected targets. The Committee was satisfied that no improper conduct on the part of CSIS contributed to the event, nor did any Service employee contravene operational policy.

The second instance related to an error on the part of the Service that had been rectified by CSIS as soon as it was noticed. Unusual and extenuating circumstances contributed to the error and the Committee is satisfied that it was unintentional. Further, the Committee was able to confirm that the Service took the proper administrative and operational measures to correct the error as soon as it became evident.

#### **Warrant Acquisition and Implementation**

With respect to all the warrants examined in both regions and based on the information made available to the Committee for review, we found that CSIS conducted the warrant acquisition process in a thorough and objective manner and used supporting information appropriately. Affidavits were complete and balanced, and the facts and circumstances of the cases were fully, fairly and objectively expressed.

The Committee also found that in executing the warrant powers obtained, CSIS exercised its powers appropriately and complied with all warrant clauses and conditions. With minor exceptions, both regions strictly observed operational policies concerning the collection and retention of information obtained under the warrants.

#### **Recruitment and Direction of Human Sources**

In all cases the Committee found that the Service had acted appropriately and within the law and had properly followed all policies and procedures relating to the recruiting and directing of human sources. In one especially sensitive area of the Service's use of human sources—one that has drawn the Committee's attention previously—the Committee found that CSIS managed the relationship with the source appropriately. The Committee did identify some minor errors and oversights in one Region's human source record keeping.

### **Interviews in the Community**

The Committee's review of relevant CSIS documentation showed that it conducted its interviews in the community in a fair and appropriate manner and with sensitivity to the interviewees' civil liberties and religious freedoms. In all the interviews reviewed, CSIS was careful to make interviewees aware that it was investigating threats posed by Sunni Islamic extremism, not investigating the Sunni community as a whole.

### **Liaison and Exchanges of Information with Domestic Agencies**

The Committee's examination showed that all exchanges of information, disclosures by the Service and joint operations were conducted in accordance with law and policy. The Service's efforts in both Regions to build strong and co-operative relationships with other agencies were evident to the Committee. In the months following the September 11 attacks, the benefit of these initiatives was especially important because available resources to investigate threats were stretched thin.

### **Issues of Internal Security**

In one region, the Committee identified a number of security violations and no breaches. In the other region, the Service had documented five security breaches: one unauthorized contact, one conflict of interest situation and three involving unauthorized disclosures. In four of the cases the Committee agreed with the measures CSIS took to mitigate possible impacts from the breaches and found that the administrative measures the Service took in relation to the employees concerned were appropriate. The fifth case remains under review by the Committee.

### **DOMESTIC THREATS IN CONJUNCTION WITH LAWFUL ADVOCACY, PROTEST AND DISSENT**

The Committee found that overall, CSIS conducted this complex set of investigations in an appropriate, lawful and professional manner, taking considerable care in implementing policy measures designed to prevent intrusion into legitimate political activity. The Committee believes, based on its investigation, that the Service took seriously its obligation to weigh the requirement to protect civil liberties against the need to investigate threats to national security.

The Committee identified a number of issues that gave rise to several recommendations.

- 1) In the case of two individual targets where it was clear that threat activities had abated, the Committee believes CSIS should have terminated its investigations earlier than it did. In addition to the general policy guidance, CSIS officers responsible for the investigation received explicit direction from management to end the investigations if no threat activities were reported.

To avoid such occurrences in the future, the Committee recommended that:

**CSIS maintain a strict awareness of operational policy and executive directive requiring the timely termination of targeting authorities in the absence of targets' threat-related activity.**

- 2) In executing valid warrant powers against an individual target, CSIS reported extensively on a non-targeted individual and collected information on that person's threat-related activities without seeking a separate targeting authority. In the Committee's view, the Service should have sought a separate targeting authority rather than rely on another investigation to collect the information it did.

Accordingly, based on this case the Committee recommended that:

**In its collection of information through the execution of warrant powers, CSIS avoid extensive reporting on non-targeted individuals, and be vigilant in seeking targeting authority once an individual's threat-related activities become evident.**

- 3) The Committee identified several administrative oversights and delays in the Service's handling of a human source file. None had any material impact on the course of the investigation or the information collected. Nevertheless, based on this case the Committee recommended that in future:

**CSIS pay strict attention to operational policy requirements regarding the administrative handling of human source files.**

- 4) The Committee found evidence of some friction in exchanges with domestic agencies. This clearly presented challenges but did not, in the Committee's view, materially impact upon the Service's effectiveness in conducting its investigations.

Accordingly, the Committee has recommended to the Service that:

**It examine whether the negotiation of co-operative agreements between CSIS and its domestic partners would be of benefit and enhance their relationships.**

#### **COLLECTION OF FOREIGN INTELLIGENCE**

The Committee concluded that in implementing ministerial requests for assistance under section 16, CSIS complied with all legal and administrative requirements.

The review identified no irregularities or other concerns regarding the authorizations for, and the management of, the collection of information under Federal Court warrants. All requests for supplementary information that CSIS sought from CSE were appropriate and in compliance with law and policy. The Committee saw no information about Canadians collected in the course of section 16 operations that had been inappropriately retained in Service files.

#### **REVIEW OF FOREIGN ARRANGEMENTS**

The Committee's review found that the establishment of the new arrangements and the expansion of the existing ones was carried out in compliance with the *CSIS Act*, ministerial direction and the Solicitor General's conditions for approval. The Committee took special care to examine information relevant to the human rights records of the agencies' host countries, including open-source reporting from reputable international human rights agencies.

In this regard, the Committee took note of several new relationships where the Service will need to exercise vigilance to ensure that no information received from an agency is the product of human rights violations, and that no intelligence transferred to an agency results in such abuses.