





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

Tel: (613) 990-8441

Fax: (613) 990-5230

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

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

© Public Works and Government Services Canada 2002

Cat. No. JS71-1/2002

ISBN 0-662-66755-7

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

September 30, 2002

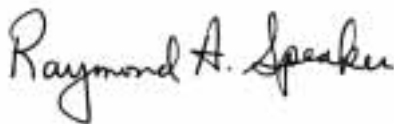
Dear Mr. MacAulay:

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 2001–2002, 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.





<b>Section 3: CSIS Accountability Mechanisms</b>	41
<b>A. Policy and Governance Frameworks</b>	43
Governor in Council Regulations and Appointments	43
2001–2002 National Requirements for Security Intelligence	43
Ministerial Direction	43
Changes in CSIS Operational Policy	43
<b>B. Reporting Requirements</b>	44
Certificate of the Inspector General for 2001	44
CSIS Annual Operational Report for 2000–2001	45
Unlawful Conduct	45
<b>C. Duties and Functions of CSIS</b>	46
Review of CSIS Domestic and International Arrangements	46
Federal Court Warrants and Warrant Statistics	48
Regulations	49
Section 2(d) Investigations	49
Disclosures of Information in the Public or National Interest	49
<b>Section 4: Inside the Security Intelligence Review Committee</b>	51
Appointment of a New Member	53
Research and Review Activities	53
Section 54 Report	53
Briefings	53
Parliamentary Relations	53
Additional Committee Activities	54
Inquiries Under the <i>Access to Information and Privacy Acts</i>	54
Budget and Expenditures	55
SIRC Staffing and Organization	55
<b>Appendix A: Acronyms</b>	57
<b>Appendix B: SIRC Reports and Studies since 1984</b>	61
<b>Appendix C: Key Findings and Recommendations</b>	71









## **Section 1**

---

### **Review of CSIS Intelligence Activities**



---

## Review of CSIS Intelligence Activities

### A. Areas of Special Interest for 2001–2002

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

A significant component of SIRC's review activity takes the form of research projects carried out by staff analysts 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 on a retrospective basis 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 Inspector General of CSIS.

Research projects for any given fiscal year are designed to yield assessments across the range of CSIS's operational activities. This approach helps ensure that the Committee delivers a comprehensive overview of CSIS's performance. A number of factors influence the selection of topics for in-depth inquiry:

- shifts in the nature of the international threat environment
- changes in technology
- need to follow up on past Committee reviews or issues arising from complaints
- significant alterations to government policy with implications for CSIS operations
- interests of individual Members.

Although the selection of research projects is approved by the Committee at the beginning of each fiscal year, the Committee has always recognized the need to adjust its review plans to respond to unexpected events. To meet the resource demands of these unforeseen reviews, the Committee maintains the capability to redirect research resources to priority issues on short notice. Our inquiry—launched in the wake of the events of September 11—into the Service's investigation of Sunni Islamic extremism, is one such example.

The review function is essentially one of risk management—deciding which areas of the Service's extensive activities warrant the most careful monitoring.

Moreover, for the first time in many years the Service is dramatically increasing its own activities in areas where SIRC has a compelling interest and legal responsibility. The Committee, together with senior staff, is currently assessing the possible implications of the anticipated rise in the level of CSIS's activities on SIRC's statutory review functions. The Committee can then develop an effective strategy, make any necessary adjustments to ensure SIRC's continued ability to meet the expectations of Parliament and the public and fulfill its statutory obligations under the *CSIS Act*.

## CSIS Investigation of Sunni Islamic Extremism

### Report # 2002-01

#### BACKGROUND

The events of September 11, 2001 in the United States made shockingly real to both the Canadian government and the Canadian public the threat of Sunni Islamic extremism. In very short order, the government took a number of administrative,

budgetary and legal measures intended to increase public safety and boost public confidence in the national security apparatus.

CSIS's investigation of Al Qaida specifically and Sunni Islamic terrorism generally was complex and of long standing

For their part, Canadians were left shaken, anxious and angered by September 11—aghast at the nature of the attacks and apprehensive about

what terrorism on such a scale might mean for daily life in Canada and the rest of the world. Underlying the national anxiety was the fear that similar attacks could have occurred in Canada or that they might happen in the future.

These worries gave rise to some serious questions: How well did Canadian authorities understand the gravity of the threat? How much did they know and how much ought they to have known about the attacks, which ultimately occurred so near to home? And finally, what are those who are supposed to guard our public safety doing to prevent future attacks here and abroad?

To begin the search for answers to these and other pertinent questions, at least insofar as CSIS is involved, the Review Committee launched a broad study of the Service's investigation of the Sunni Islamic and Al Qaida terrorist threat to

Canada prior to and around the time of the September 11 attacks. Past Committee reviews have explored various aspects of the Service's role in counter terrorism in general, and Sunni Islamic terrorism in particular, so the area is not new for the Committee.

### OBJECTIVES AND METHODOLOGY

The Committee recognized from the outset that CSIS's investigation of Al Qaida specifically and Sunni Islamic terrorism generally was complex and of long standing. The Committee's inquiries for this study were therefore chiefly informational in nature, designed to survey the Service's activities in the months leading up to September 11—information and analysis we regard as prerequisites for any additional examinations.

None of the advice warned of a threat sufficiently specific in time or place to have alerted government authorities to the events of September 11

The objectives of this overview study were fourfold:

- 1) to gain a broad understanding of the reach and focus of the Service's investigation of Sunni Islamic extremist activities;
- 2) to determine the nature and quantity of assessments, analyses and other forms of advice about the threat transmitted by CSIS to relevant government and law enforcement clients;
- 3) to review the character and quantity of information exchanges about Sunni Islamic extremist activities with the intelligence services of allied nations; and,
- 4) to identify subjects meriting further study by the Committee.

The nature of the Committee's inquiries necessarily influenced the sorts of conclusions that we drew from the information reviewed. For example, the Committee did not examine all the raw intelligence collected by the Service or passed to it from other agencies. Nor did we review specific warrants or delve into the handling of individual human sources with a view to ensuring compliance with law and policy.

Instead, the Committee's focus in this study was on examining material that would aid in understanding how the Service ran its investigation, who its chief

## Sunni Islamic Extremism and the Al Qaida Movement

Following are excerpts from CSIS publications written prior to September 11 on the subject of the Al Qaida terrorist organization and Sunni Islamic extremism generally:

"Most identifiable groups in the Islamic Movement [radical Islamic fundamentalists] of the Middle East and elsewhere share the common objective of creating a truly Islamic society in which they can live under a regime governed by the rules of their faith as codified in Islamic law.... Some much smaller subsets are those Islamic groups which promote a genuinely radical political agenda through the avenue of violence."

"Interpretations of the *Qur'an* vary and there are many different schools of legal interpretation within Sunni Islam. Struggle or *jihad* to attain this goal is a central tenet of Islam, but is also multivariied and can mean anything from internal struggle to fight evil from within to 'holy war' in the literal sense which is how the Islamic militants utilize this term. *Jihad* is used to give religious sanction to violence against 'unbelievers' or *kafir* (atheists) who can range from non-Muslims to other Muslims who disagree with the militant philosophy."

"Muslim terrorists are often Mujahadeen, 'holy warriors', devoted to Islam and committed to *Jihad*, ('Holy War'), possessing combat experience of such locations as Afghanistan, Bosnia, and Chechnya. Well schooled in handling weapons, explosives and communications equipment, they know the value of the Internet, fax machines, cellular telephones and encryption. Increasingly sophisticated and willing travellers, they have access to excellent false documentation and international contacts, and can blend easily into a local émigré community, where they can execute attacks without being readily identified. It is their nebulous, unstructured characteristics, combined with zealous dedication, which contribute in large measure to the menace they present."

"The Al Qaida organization is a structured component at the heart of the terrorist network led by Osama Bin-Laden. It functions as an umbrella organization, with branches in the Middle East, Africa, and Central Asia, and operates terrorist training camps located in Afghanistan. Graduates from the camps have been dispatched to various hot spots around the world to support a variety of Islamic extremist groups and causes. It is assessed that Al Qaida may have up to several thousand members."

"The Service deems Islamic extremists as the largest danger in terms of religious terrorism. In part an outcome of magnitude of numbers and Islam's global reach, it is also because unlike the cohesive groupings of the past, many militant Islamists are individuals who do not owe allegiance to any particular organisation, making identification and trace checks very difficult."

interlocutors were, the analytical outcomes generated by the intelligence it collected and the content of the Service's advice to government. We also inquired into how CSIS adapted to the immediate crisis created by the September 11 events with respect to the redeployment of human and technical resources.

The Committee's review covered the period April 1, 2001 through September 12, 2001. However, to complete our investigation we examined additional documents and relevant data that fell outside the formal review period.

### **FINDINGS OF THE COMMITTEE**

The Service's investigation of Sunni Islamic extremism is a long-standing one and has grown steadily in scope and complexity since its inception. At the time of the September 11 attacks, the Service's investigation of Al Qaida appears to have been extensive.

Through all manner of intelligence gathering—direct and indirect—CSIS appears to have run an aggressive investigation. It managed human sources, obtained and implemented Federal Court warrant powers and exchanged intelligence with allied agencies.

With respect to making use of this information to advise government, CSIS was active as well. Since the beginning of the investigation, the Service has disseminated to government departments and law enforcement agencies numerous publications and intelligence advisories (most of them classified) on the matter of Sunni Islamic extremism—almost half of them in the more recent past. In addition, CSIS gave numerous briefings and presentations to government dealing wholly or in part with Sunni Islamic terrorism.

Based on our examination, the Committee believes that the Service disseminated widely within government timely information about the potential for Sunni terrorism. Although none of the intelligence products or threat warnings we reviewed pointed directly to the events of September 11, the Service clearly was aware of the potential for Al Qaida-inspired terrorist attacks of some kind and communicated this information to the appropriate bodies in government. In the Committee's view, however, none of the advice or communications the Committee reviewed warned of a threat sufficiently specific in time or place to have alerted government authorities to the events of September 11.

## CONCLUSION

From the information and documentation we reviewed, the Committee concluded the following:

- CSIS has for some time been actively seized with the issue of Sunni Islamic terrorism and continues to investigate this threat aggressively.
- In its duty to advise government, CSIS acted in a timely manner to tell government what it knew of the Al Qaida/Sunni Islamic threat.
- In the wake of September 11, the Service continued to deploy human and technical resources with the aim of countering this and related threats.

In carrying out this overview study, the Committee has laid the foundation for future in-depth inquiries into specific elements of the Service's Sunni Islamic extremist investigation. We will elaborate on our findings in future reviews and annual reports.

## Source Recruitment

---

### Report # 2001-01

---

#### BACKGROUND

Human sources are an extremely valuable tool in the Service's gathering of intelligence about potential threats to Canada. Clearly, the recruitment of sources is a sensitive area of CSIS's operations. Thus a considerable amount of Ministerial Direction and Service policy is devoted to ensuring that all operations involving human sources are managed appropriately and within the law.

This study arose from Committee findings in a previous complaint case. Our report on the complaint identified several shortcomings in the Service's procedures and the Committee expressed its intention to undertake a follow up review at a future date. The goal of this study was to re-examine the Service's source recruitment practices in this most sensitive area.

#### METHODOLOGY

The Committee's review drew on a sample of cases that met the study criteria between October 1999 and September 2000. We examined all relevant electronic and hard-copy documentation related to each case and measured these against

current Service policies and procedures for source recruitment. The policies were themselves examined to determine their effectiveness. The Committee also interviewed the relevant CSIS senior officials in charge of the source recruitment program.

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

Overall, the Committee found that the human source operations we reviewed were carried out in conformity with law, Ministerial Direction and policy. Those files we examined showed that the Service conducted itself appropriately and in accordance with policy adjustments made in the wake of the Committee's previous report. The Committee also determined that the Service had assessed the reliability of the sources with appropriate caution and that all transactions we reviewed complied with established policies.

The Committee's review did identify two administrative shortcomings in the management of the source files: first, in a few instances, inadequate record keeping; and second, Headquarters approval necessary for a particular activity was not obtained in a timely manner. With the aim of avoiding similar difficulties in the future, the Committee made two recommendations to CSIS, which for reasons of national security cannot be elaborated here.

Given the potential for misunderstanding, the Committee stressed to the Service that it should continue making every effort to ensure that sources are fully aware of the nature of their relationship with the Service. The Review Committee will continue to monitor the Service's activities in this especially sensitive area.

## **Domestic Extremism**

---

### **Report # 2001-03**

---

#### **BACKGROUND**

For more than a decade, CSIS has conducted periodic investigations in this area on the basis that the activities being investigated represented threats to public safety and to national security. In light of the sensitivity of the subject and the need to ensure that the rights to legitimate advocacy, protest and dissent were not being in any way infringed, the Committee has monitored the Service's activities closely.

This study is one of several examinations by SIRC of the Service's activities in the area. As in previous cases, the aim was to determine whether the Service had reasonable grounds to suspect that the activities of the targeted groups and

individuals represented threats to the national security of Canada; whether the Service recruited and managed human sources appropriately; and, whether CSIS acted in compliance with the *CSIS Act*, Ministerial Direction and relevant operational policies. The Review Committee also reviewed the nature of the Service's co-operation with federal and provincial departments of government and law enforcement agencies.

#### SCOPE AND METHODOLOGY OF THE AUDIT

The Committee reviewed all relevant Service documents and files (electronic and hard-copy) for the period April 1998 through September 2000. These documents included but were not limited to targeting authorizations, warrants and their supporting documents, operational reports, human source logs, internal CSIS correspondence and records of exchanges of information with other agencies and departments.

Information gathered in the course of the investigation helped to minimize the potential for serious violence

#### FINDINGS OF THE COMMITTEE

##### Targeting and Investigations

The Service issued two targeting authorities related to this issue during the period under review: one was issue-based; the other focused on a particular organization. The Committee reviewed all the relevant files and randomly selected individual targets investigated under the two authorities. For each case, the Committee posed three basic questions:

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

With respect to the investigations conducted under the issue-based authority, the Committee found that the Service had reasonable grounds to suspect an imminent threat of politically motivated violence; that the level of the investigations was appropriate to the nature of the threat; and, that all information reported met

the “strictly necessary” test. The Committee’s research found no extensive reporting on individuals who were not engaged in threat-related activities.

The records also show that the Service exercised the issue-based authority judiciously, terminating investigations when it determined that individuals did not pose a threat. Overall, CSIS appeared sensitive to the need to distinguish between threat-related activities and legitimate political ones. (*see* inset “Issue/Event-based Targeting”.)

The second targeting authority the Committee reviewed named a particular organization. Here too, the Service conducted its investigations in an appropriate and lawful manner. It was clear to the Committee that in one specific instance,

### Issue/Event-based Targeting

This type of targeting authorizes CSIS to investigate in circumstances where it 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. The targeting authority allows CSIS to investigate the general threat and to try to identify the persons or groups who are taking part in threat-related activities. As in any other targeting procedure, if warrant powers are involved, approval must be granted by the Federal Court.

In his 1995 Certificate, the then Inspector General of CSIS expressed reservations about the breadth of issue-based investigations. In his view they held the potential to involve entire communities and to permit the Service to collect and retain a wide assortment of personal and other information on individuals and groups not themselves mandated CSIS targets. The Service disagreed, stating that investigations only commenced when the “reasonable grounds to suspect” standard, which is applicable to all mandated investigations, had been met.

The Review Committee shares concerns that issue/event-based investigations could encompass persons and groups who are not targets. However, as we wrote on the subject in our 1998–99 Report:

[T]here is a place for issue-based targeting in the array of options legally available to CSIS... [with] the caveat that 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 each of these investigations case-by-case as we encounter them so as to assure ourselves that they are being conducted appropriately.

information gathered in the course of the investigation helped to minimize the potential for serious violence.

The Committee's only reservation arose from a review of information collected under the targeting authority in the year prior to its expiration. In the Committee's opinion, most of the data concerned activities by the target that were not threat-related. It was evident to the Committee that the organization no longer posed a threat of politically motivated violence as defined under section 2(c) of the *CSIS Act*. It is the Committee's view that the Service should have considered terminating the investigation before the mandated expiry date. In response to our concerns, the Service stated that it required the full 12 months of investigation to assess accurately the group's potential for engaging in politically motivated violence.

#### Human Source Operations

Such is the sensitivity of human source operations that they are the subject of special Ministerial Direction, detailed policy requirements and regular scrutiny by CSIS senior management. Historically, the Committee, in any investigation it reviews, has looked closely at the manner in which the Service complies with these rules.

In connection with our review of the Service's investigation, the Committee selected a number of human source cases for extensive audit. In each case, the Committee was satisfied with the Service's recruitment and direction of the source and found CSIS to have been diligent in complying with operational policy requirements.

#### Inter-agency Co-operation

The objective of this part of our review was to assess the quality of the co-operative relationship on this investigation between CSIS and other relevant agencies—specifically, federal and provincial departments of government and law enforcement bodies.

Overall, the Committee found the nature and level of co-operation between the Service and other domestic agencies to be both appropriate and productive. The Committee took special note of the high level of information sharing between CSIS and the RCMP.

The Committee will continue to pay close attention to all the Service's activities in this area and intends to revisit the investigation regularly.

## Collection of Foreign Intelligence

---

### Report # 2001-05

---

#### METHODOLOGY

The Committee's review encompassed all Ministerial requests for assistance, all section 16 information retained by CSIS for national security purposes and all exchanges of information with the Communications Security Establishment (CSE) in the context of foreign intelligence gathering. Besides this material, which is regularly subject to Committee scrutiny, we reviewed a random sampling of feedback from Service clients on section 16 intelligence products.

The goal of the audit was to:

- Review 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 Memoranda of Understanding (MOUs).
- Examine the nature of the relationship between CSIS and CSE as it relates to section 16 matters to ensure that it complies with the law, Ministerial Direction and operational policy.
- Understand the role of client feedback in how the Service prepares intelligence products for its clients in government.

#### FINDINGS OF THE COMMITTEE

##### Requests for Assistance

All Ministerial requests under section 16 complied with the necessary legal and administrative requirements. For the period under review, no new legislative, policy or judicial guidelines were issued in relation to activities under section 16.

##### Warrant Implementation

The Committee examined a selection of warrants directed at section 16 collection including all related working files, affidavits and logs. We also interviewed relevant Service officers. In each of the cases reviewed, we found the collection activities were correctly administered and identified no instances of non-compliance with law or policy.

### Requests for Identifying Information

Information that CSE gives to the Service is routinely “minimized” to comply with various prohibitions against targeting Canadian nationals and Canadian businesses. Under specific circumstances, the Service may request identification from CSE 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*. In its review of these requests for supplementary information, the Committee determined that all complied with law and policy. We saw no information about Canadians collected in the course of section 16 operations that was inappropriately retained in Service files.

### Access to Section 16 Information

Given the extremely sensitive nature of section 16 operations, access to the database containing this information is restricted to only those CSIS employees who have received special clearance and indoctrination. The database is thus not normally accessible to intelligence officers involved in investigations under section 12. The Committee reviewed random samples of correspondence related to the indoctrination of intelligence officers requiring access to this database and their requests for access. We found all requests and reports examined to be appropriate.

### Client Feedback

Client assessment of intelligence product is an essential part of the intelligence cycle. The Committee examined a sampling of client assessments received by the Service during the period under review and found that the Service appeared to weigh all such feedback carefully and make adjustments where appropriate.

## Background to Section 16 Collection of Foreign Intelligence

Foreign intelligence is defined as any information about the capabilities, intentions or activities of a foreign state, foreign national or foreign organization (including commercial enterprises) collected in Canada. 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.

### *History*

In the first few years after CSIS was created in 1984, little use was made of section 16. In 1987, the ministers of External Affairs and National Defence, and the Solicitor General signed a MOU. A classified document, the MOU sets out exactly how the provisions of section 16 will be exercised, the means to authorize and conduct section 16 collection and the roles and responsibilities of

---

*(Background continued)*

---

all concerned parties including the Review Committee. In 1990, a second MOU was concluded between the Service and the Communications Security Establishment (CSE) elaborating on the earlier agreement.

***Procedures***

Under the provisions of section 16, either the Minister of National Defence or the Minister of Foreign Affairs 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 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 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 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.

## CSIS Liaison with Foreign Agencies: Audit of an SLO Post

Report # 2001-04

### BACKGROUND

Security Liaison Officer (SLO) post audits address the Committee's obligation, under section 38(a)(iii) of the *CSIS Act*, to examine the Service's performance of its duties and functions in connection with arrangements with foreign governments and institutions thereof. By focusing on a single CSIS security liaison post,

The SLO post was effectively managed and its staff held in high regard by the senior staff of the mission

the Committee is able to review the Service's relations with foreign security and intelligence agencies, the management of controls over the dissemination of CSIS information, post profiles and foreign agency assessments prepared by the SLO and the nature of the

information collected and disclosed. The audit also allows the Committee to identify developments, pressures and emerging issues specific to the post and the foreign agencies within the post's ambit.

This year the Committee selected a post whose existence predates that of CSIS. International events and intelligence activities of mutual interest to the Canadian government and host country helped influence our choice. Also, last year's SLO post audit pointed to this particular post, among others, as having an especially heavy and expanding workload. The Committee wished to review the situation first-hand.

### METHODOLOGY

As with all Committee SLO post audits, the essential goals were twofold: first, to ensure that relationships and contacts with foreign agencies complied with the specific arrangements that govern them; and second, to monitor the controls over information disclosed to foreign agencies or received from them. More broadly, the activities of the selected post for the period under review—April 1, 1999 through March 31, 2001—were examined in the context of the *CSIS Act*, Ministerial Direction and CSIS operational policies.

At CSIS Headquarters (HQ) the Committee reviewed:

- post profiles and assessments of foreign agencies prepared and updated by the SLO;

- liaison arrangements with the foreign security and intelligence agencies covered by the post; and,
- the information and intelligence exchanged between HQ and the SLO.

At the post we examined:

- the content and scope of correspondence released by the post to foreign security and intelligence agencies; and,
- a sample of the files relating to the Assistant Security Liaison Officer's (A/SLO's) assistance to Citizenship and Immigration on security assessments of applicants for landed immigrant status.

The Committee's on-site review also included interviews with the SLO and A/SLO, the resident RCMP liaison officer, senior staff of Citizenship and Immigration Canada (CIC), Canada's Head of Mission and the Mission's Counsel General.

## FINDINGS AT THE POST

### Overview

Our observations, reviews of documentation and interviews all led the Committee to conclude that the SLO post was effectively managed and its staff held in high regard by the senior staff of the mission. Unlike the substandard conditions identified in last year's SLO post audit, the Committee saw no deficiencies in either the physical facilities or the security arrangements.

One reason why the Committee selected this post for audit was its pivotal role in events of mutual interest to the Canadian and host country's security services. Actions by the security intelligence and law enforcement agencies of both countries, before and after these events, directly affected the character and volume of exchanges handled by the post. For the Committee, the exchanges provided additional insight into the greater demands being placed on the Service's relationships with other intelligence agencies.

### Workload

During the two years under review, heavy workloads at the post necessitated repeated requests to CSIS HQ for temporary, additional resources to address administrative and operational backlogs. The Committee concluded that the

work backlogs were neither the result of inefficiencies nor were they one-time events. Rather they arose from the consistently high demands made of the SLO post staff. In the Committee's view, the Service may wish to reconsider whether short-term, temporary staff assignments are indeed the most effective way of dealing with this ongoing situation.

#### Visits to the post

The Committee also followed up on the concern expressed at CSIS HQ that the planning of a large number of visits to SLO posts for the purpose of meeting with

foreign agency counterparts imposed an undue organizational burden on the SLOs who had to coordinate the visits. The SLO at this post stated that, to the contrary, well-organized meetings of visiting Service officers with their counterparts generated an increase in the exchanges of information and contributed positively to the overall

The exchanges provided insight into the greater demands being placed on relationships with other intelligence agencies

credibility of the liaison program. The Committee's review of the available records, as well as feedback from foreign agencies provided to CSIS HQ, all bore out the SLO's assessment.

#### Information exchanges

The Committee examined both the documentation prepared for disclosure by the SLO to foreign agencies and the information exchanged between CSIS HQ and the post. The information reviewed included exchanges of intelligence and that dealing with operational co-operation. In preparing CSIS information for disclosure to foreign agencies, the SLO must follow specific administrative procedures. With only a few minor exceptions, all the disclosures prepared by the SLO complied with these procedures. The Committee found that the remaining exchanges of information between CSIS HQ and the SLO post, and information disclosed by the SLO to foreign agencies, were in compliance with the *CSIS Act*, Ministerial Direction, operational policy and the relevant foreign arrangements.

#### Co-operation with Citizenship and Immigration

Another issue raised in last year's SLO post audit, which the Committee intended to revisit, was that of SLO assistance to CIC in the form of immigration screening. Last year's study cited Service senior management as sharing Committee concerns that the overburdening of SLOs with immigration matters, which we identified at one post, in fact extended to certain others, including the post reviewed here.

## CSIS Foreign Liaison Program

### *Ministerial Direction and Policy*

The authority to enter into arrangements with foreign governments and international organizations and their intelligence agencies is provided by the *CSIS Act*. The specific rules and functions governing foreign liaison activities at SLO posts are set out in Ministerial Direction and CSIS operational policy. Service operational policy describes the roles and functions of SLOs, whereas Ministerial Direction outlines requirements for new and existing foreign arrangements.

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 and International Trade;
- the Director 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.

### *SLOs and the Foreign Liaison Program*

The role and functions of the SLOs are to:

- maintain and develop channels of communication with foreign agencies with which the Service has approved arrangements;
- carry out security screening activities in support of the Immigration Screening program;
- report to CSIS headquarters on any matter related to Canadian security interests; and
- undertake specific reliability checks as requested by the Mission Security Officer.

The Committee's examination of records this year showed that temporary assistance to the post was provided by the Security Screening Branch in each of the last three calendar years. The SLO noted to the Committee that requests to HQ for temporary assistance have, to date, always been granted.

It was evident to the Committee that the growing volume of work posed challenges that continue unabated. During on-site interviews, CIC staff advised

the Committee that their referrals for immigration security screening to the Service were greater than at other CIC offices abroad. As with the more general issue of workload at SLO posts, the Committee believes the Service may need to reconsider whether temporary staff assignments are the best means of handling the growing workload. It is important to note that, notwithstanding the demands imposed by the immigration security screening program, the Committee saw no evidence that the post was failing to meet its obligations.

#### Foreign Agency Assessments

In past reviews, the Committee has emphasized the importance it places on the Service's responsibility to take all possible care to ensure that the information it

Notwithstanding the demands of the security screening program, the Committee saw no evidence that the post was failing to meet its obligations

exchanges with foreign agencies is not used in ways that could result in violations of human rights. The SLO is responsible for regularly updating assessments of foreign agencies and promptly submitting these to CSIS HQ. The agencies are assessed both for their human rights records and their propensity to pass information

on to third parties without authorization. After reviewing the agency assessments prepared by the SLO post, the Committee was satisfied that they were complete and properly carried out.

## Warrant Review

### Report #2001-06

#### BACKGROUND

A warrant issued by the Federal Court of Canada is the legal mechanism by which CSIS is authorized to exercise its most intrusive powers in the course of investigating threats to the security of Canada. The legislative mandate for Federal Court warrants is found in section 21 of the *CSIS Act*, which allows the Service to obtain warrants to assist in its investigations of threats to the security of Canada.

By regularly examining a sample of cases in which CSIS has acquired and implemented warrant powers, the Committee gains insight into the Service's core investigative activities. From among the warrants issued in 2000–2001, the

Committee selected one counter terrorism warrant and one counter intelligence warrant. Each case was examined from two perspectives: first, the Service's activities in acquiring warrant powers from the Federal Court; and second, the manner in which CSIS implemented those warrant powers. The overall objective was to ensure that all the Service's activities complied with the *CSIS Act*, Ministerial Direction and operational policy.

## METHODOLOGY OF THE AUDIT

### Warrant Acquisition

In reviewing the Service's acquisition of warrant powers, the Committee examined all documents relating to how the warrant applications were prepared, including the affidavits; supporting documentation used to substantiate the affidavits; the working files related to the affidavits; the Requests for Targeting Authority; and the Target Approval and Review Committee (TARC) minutes.

The purpose of reviewing the documentation on how the Service acquires warrant powers is to ascertain whether

- the allegations in the affidavits are factually correct and are adequately supported in the documentation;
- all pertinent information is included in the affidavits; and,
- the affidavits are complete and balanced, and the facts and circumstances of the cases are fully, fairly and objectively expressed.

### Warrant Implementation

In reviewing how the warrant powers were implemented, the Committee examined the warrants themselves; the Service's regional and headquarters warrant administration files; all regional files concerning warrant implementation and sensitive operations; and electronic operational reports pertaining to the targets of the warrants. The purpose of the review is to assess the Service's use of the powers granted by the Federal Court and to determine whether CSIS complied with all clauses and conditions contained in the warrants.

## FINDINGS OF THE COMMITTEE

The Service's procedures for managing warrants through the entire life cycle of acquisition and implementation are both exhaustive and complex. In reviewing

## The Warrant Process

To obtain warrant powers under section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court with a sworn affidavit that sets out the reasons why such powers are required to investigate a particular threat to the security of Canada. Preparing the affidavit is a rigorous process that involves extensive consultations with the Department of Justice and the Solicitor General, with the latter's approval being required before a warrant affidavit is submitted to the Court. The facts used to support the affidavit are verified during the preparation stage and reviewed again by an independent counsel from the Department of Justice to ensure that the affidavits are legally and factually correct prior to their submission to the Federal Court.

both the counter terrorism and the counter intelligence warrants, the Committee found that, on the whole, the Service managed each warrant properly and complied with both the *CSIS Act* and Ministerial Direction.

### Warrant Acquisition

The Committee found that CSIS managed the warrant applications in a thorough and objective manner, although there were several minor instances in which the affidavits were not consistent with the supporting documentation. While none of the errors were material in nature, the Committee believes strongly that CSIS must continue to pay scrupulous attention to its affidavit drafting procedures. Accordingly, the Committee recommended that,

**CSIS should strive for the utmost rigour in its warrant acquisition process, ensuring that allegations in the affidavit are factually correct and adequately supported in the documentation.**

### Warrant Implementation

With respect to how the Service complies with its own operational policy requirements and administrative practices, we identified a number of shortcomings in how one warrant was implemented. Although none materially affected the overall management of the warrant, the Committee made four recommendations to the Service designed to avoid future problems. Two were recommendations to amend or clarify specific policies so that they could be implemented more consistently. A third spoke to the need for the Service to adhere more consistently to a specific existing policy.

Giving rise to the fourth recommendation was an instance in which a particular administrative oversight had the potential of creating the perception that the Service was implementing warrant powers after the warrant had expired. Although

the Committee determined that the warrant was properly managed by the regional office concerned, we did recommend to the Service that it adopt a new administrative procedure that would eliminate the potential for ambiguity.

#### The “Strictly Necessary” Test

For both warrants reviewed, the Committee found that CSIS adequately justified its choice of information collected and retained and in general met the “strictly necessary” test set out in section 12 of *CSIS Act*. However, the Committee identified a small number of instances where CSIS collected personal information that the Committee felt was of questionable relevance to the targets’ threat-related activities. The Service disagreed with our observation.

We did recommend to the Service that it adopt a new administrative procedure that would eliminate the potential for ambiguity

Given the centrality of the “strictly necessary” test to the integrity of the intelligence gathering process, the Committee felt prompted to make a formal recommendation. Accordingly, the Committee recommended that,

**CSIS should maintain a strict awareness of the conditions stated in Federal Court warrants and of the “strictly necessary” test outlined in section 12 of the *CSIS Act* so that its collection of information continues to meet legal and policy directives.**

## B. CSIS Reporting on Operational Activities

### 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 a political, religious or ideological objective continues to be one of the Service's chief priorities.

As discussed in some detail in the Committee's study of CSIS's investigation of Sunni Islamic extremism (*see* pages 4–8), the threats represented by Sunni extremists have been and remained in 2001–2002 a major priority for the CT Branch. CSIS reported no significant changes in operational focus or priorities

in the year under review. Reporting on the threat of terrorism more generally, the Service continues to regard the spread of advanced communication technologies, the ease and speed of international travel and the diffuse nature of terrorist alliances as its greatest challenges. In the Service's view, these factors have rendered "geographic constraints to the spread of terrorism . . . virtually non-existent."

### 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.

CT Threat Assessment Unit produced 795 assessments for government clients—a considerable increase over the previous year's 544

In 2001–2002, the CT Threat Assessment Unit produced 795 assessments for government clients—a considerable increase over the previous year's 544. CSIS attributed the increase to three factors: first, a greater

number of special events (for example, major conferences and diplomatic events); second, increased demand from various departments of government; and third, its own more "proactive stance" to issuing assessments.

## 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 the CI Program continues to change with the evolving geopolitical environment.

The Committee had asked the Service for information regarding the impact of the events of September 11 on the CI Branch. The Service provided detailed information to the Committee on the effect of the events of September 11 on the CI Branch's operational activities and deployment of resources. The Service reported on a number of active and successful investigations across the spectrum of CI's activities.

## Research, Analysis and Production

As the research and analysis arm of CSIS, the Research, Analysis and Production Branch (RAP) 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 and where 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 sections 19(2)(a) through (d) of the *CSIS Act*—are another means by which RAP disseminates intelligence product. RAP reported that in 2001–2002 there were 778 section 19 disclosure reports, a dramatic increase over previous years: namely 307 in 2000–2001 and 101 in 1999–2000.

According to the Service, the rise in numbers was the result of greater sensitivity of CSIS officers in Canada and abroad to section 19 issues, and documents being more effectively disseminated by foreign intelligence services in accordance with exchange arrangements.

In 2001–2002, RAP also produced 83 classified reports compared to 93 the previous year. RAP's intelligence publications generally fall under two categories:

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

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 eight IAC reports. These reports are distributed to a senior readership across government.

## 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 Citizenship and Immigration Canada's decision to admit an individual into the country and in granting either permanent resident status or citizenship.

### SECURITY SCREENING FOR FEDERAL EMPLOYEES

#### 2001–2002 Key Statistics

- The Service received 65 066 requests for security screening assessments for clearance, levels one through three, new upgraded and updated. This number represents a substantial increase from 36 803 in 2000–2001. CSIS attributed the increased volume to government client concern following the events of September 11 and extra prudence in the context of Canadian military operations in the Afghan theatre of operations. Also, 312 requests were for action relating to administrative procedures such as transfers and downgrades.
- This year, CSIS reported on median turnaround times for security screening assessments in two separate categories—DND and Government (*see* Table 1). The Service reported that administrative practices in the client departments accounted for the discrepancies between screening times for DND requests and those for the rest of the government.
- The Branch reported that it had improved turnaround times, which it attributed to government clients expanding their use of the Electronic Data Exchange (EDE). CSIS expects the trend to continue as almost all government departments will have switched to EDE by the end of fiscal year 2002–2003, obviating the need to handle about 6000 cases per year by hand.
- The Service reported that they had completed 4000 government security screening investigations and that another 1376 were still ongoing. Of these

**Table 1**  
**Security Screening Turnaround Times**

Category	Level	Median length of time (in days)
DND	1 (Confidential)	43
	2 (Secret)	50
	3 (Top Secret)	97
Government	1 (Confidential)	2
	2 (Secret)	30
	3 (Top Secret)	62

requests, the largest number came from the Department of National Defence, followed by the Communications Security Establishment, Canadian Security Intelligence Service, Department of Foreign Affairs and International Trade, Public Works and Government Services, the Privy Council Office and Citizenship and Immigration Canada.

- The Service reported that they received 33 108 requests for assessments under the Airport Restricted Access Area Clearance Program (ARAACP). This number represents a 10.8-percent decrease in requests for security assessments reported by CSIS last year, because the Service completed most of the clearances required for this program in the previous fiscal year. The median turnaround time for ARAACP requests is 15 days.
- There were 20 803 requests for security assessments related to “site access,” of which only 2954 were from federal government clients. The significant increase in the number of these security assessments is attributed to the fact that the Canadian Nuclear Safety Commission enacted order #01-1 on October 19, 2001 for enhanced security measures, including security screening by CSIS of all employees at nuclear power facilities.
- The Service reported that their security screening investigations resulted in 26 information briefs and one denial brief.
- With the RCMP acting as intermediary, the Service received 214 requests for accreditation to access the Parliamentary Precinct and 16 781 requests for accreditation to special events and functions to which access is controlled.

### 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 section 19 of the *Immigration Act*.

### 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 2001–2002, the Service received 45 902 such screening requests.<sup>1</sup> Of these requests, 26 735 were immigration applications and 12 226 came through the Refugee Determination Program.

The time required for the Service to issue its recommendations based on an immigration application differs considerably based on how the application was filed. Those applications filed using the EDE took a median of 77 days, whereas those filed on paper took a median of 159 days. The average number of days for the Service to respond was 86.

### 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 (IPM) or upon receiving adverse information about a case from established sources. This division of labour allows the Service to concentrate on the higher-risk cases.

In 2001–2002, the Service received 28 775 requests to screen refugee and immigration applications initiated outside of Canada. Of these, CSIS reported that 7155 were referred to SLOs for consultation.

### NATURE OF CSIS ADVICE TO CIC

Immigration requests for security screening resulted in 415 briefs from CSIS to CIC—282 inadmissible briefs and 133 information briefs. Of those requests, the

---

1. This number includes the 6941 cases that originated from the United States, an increase of 1624 from 2000–2001.

## HOW CSIS PROVIDES ADVICE TO CITIZENSHIP AND IMMIGRATION CANADA

CSIS is solely responsible for providing security screening assessments for immigration applications originating in both Canada and the United States. For immigration applications originating elsewhere, it is up to the Immigration Program Manager (IPM) at the Canadian overseas mission concerned to request a security screening assessment. In either case, regardless of the advice CSIS gives to CIC, the final decision on any potential immigrant's admissibility rests with the Minister of Citizenship and Immigration.

A typical investigation begins when the Service receives a request for immigration security screening from either a Case Processing Centre in Canada or an IPM at a Canadian mission overseas. The investigation ends when the Service provides its 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 of inadmissibility outlined in the security provisions of section 19 of the *Immigration 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 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 nonsecurity-related activities described in section 19 of the *Immigration 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*.

average time required for a “no reportable trace” (NRT) was 55 days, for an information brief 401 days and for an inadmissible brief 498 days. In the latter two categories, the figures represent a significant improvement over the previous year, which were 661 days and 644 days, respectively. For applications under the Refugee Determination Program, information briefs required 355 days on average and inadmissible briefs 433 days.

The Service reported reduced turnaround times for security screening assessments as compared to the previous year. This improvement is attributed to the fact that more clients are using the EDE software, including several foreign immigration posts. Also, the Service sent 50 “incidental letters” to CIC.

#### **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, NS. The names of citizenship applicants are cross-checked against the names in the Security Screening Information System database. The Service maintains a Watch List, which is made up of individuals who have come to the attention of CSIS through, *inter alia*, TARC-approved investigations.

In 2001–2002, the Service reviewed 144 346 citizenship applications for CIC. Of these, 2 resulted in inadmissible briefs and 129 in information briefs. In 10 instances the Service sought Ministerial approval to defer its advice.

#### **FRONT-END SCREENING PROGRAM**

The Front-End Screening Program is a recent government initiative through CIC, to ensure that all refugee claimants arriving in Canada are subject to a screening process similar to that for applicants for permanent residence. The aim of the program is to identify potential security and criminal cases in the refugee claimant stream as early as possible in the determination process.

In the four months of operation, between November 25, 2001 and March 31, 2002, the Service received 5522 cases from CIC for processing.

#### **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 2001–2002, the Service reported that 1908 screening checks were done on behalf of foreign agencies. Of these, 91 resulted in either field investigations, information briefs or recommendations for rejection. These statistics compare to last year’s 995 and 66, respectively.

Three reasons were given by the Service to explain the sharp rise. First, following the events of September 11, the demand for security screenings increased in all categories; second, requests for foreign agency screenings typically increase during any year in which the Olympic Games are staged; and third, the Screening Branch cleared a backlog of immigration cases late in the fiscal year under review.

## CSIS Funding Following Events of September 11

In its December 2001 budget, the government allocated an additional \$7.7 billion for the purpose of enhancing the personal and economic security of Canadians. Of this total, \$1.6 billion was to augment the nation's capacity for intelligence-gathering and policing. Beginning almost immediately after the events of September 11 and extending into future years, CSIS received authorities for increased spending of 30 percent for fiscal year 2001–2002 with smaller increments in subsequent years. By fiscal year 2006–2007, the Service's budget will have increased by 36 percent over the level in fiscal year 2000–2001.

Beginning almost immediately after the events of September 11, CSIS

The Committee sought and received briefings and other detailed, classified information from the Service on various elements of its spending plans. The

received authorities for increased spending of 30 percent

Service intends to increase its staff complement by 283 full-time positions and channel more resources to carrying out the increased volume of security clearances for various government clients. The new funds will also be used to upgrade and replace technical equipment and information systems.

On how it intends to use its new resources, CSIS stated in its most recent public annual report:

The additional resources, both human and financial, will allow the Service to broaden its daily activities and inject more flexibility into its choices of intelligence operations. Priority investigations will be maintained and areas reduced to address the priority threat will return to a full investigative posture.<sup>2</sup>

The Committee will continue to inform itself on the issue as the new funds come on stream in future years.

---

2. *CSIS 2001 Public Report*, Ottawa, 2002, p. 18.



## Section 2

---

### Investigation of Complaints



## Investigation of Complaints

### Complaints Case Histories

This section summarizes complaint cases submitted to the Review Committee on which decisions were reached during the past year. Not addressed here are complaints that were handled through administrative review, were misdirected or were deemed to be outside the Committee's jurisdiction. The summaries are edited to protect the privacy of complainants and to prevent disclosure of classified information.

Where appropriate, complaints are investigated through quasi-judicial hearings presided over by a Member of the Committee. After the hearings are complete, the presiding member issues a report 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.

Pursuant to the *CSIS Act*, the Committee reported on seven complaint cases reached during the period under review: three were complaints lodged in accordance with section 41—"any act or thing"; two were section 42 complaints (denial of security clearance); two were referrals from the Canadian Human Rights Commission (CHRC) (*see* Table 2).

**Table 2**  
**Disposition of Complaints\***

Status of Complaints and Reports	1999–2000	2000–2001	2001–2002
Carried over	20	24	41
New	55	52	45
<b>Total</b>	<b>75</b>	<b>76</b>	<b>86</b>
Closed	51	35	69
Carried forward	24	41	17
Orders and reports arising from complaints	4	3	16

\*Table 2 reflects all complaints received by the Committee. Not all complaints received require further inquiries by the Committee nor does every complaint result in an investigation.

## Reports of Decisions

### SECTION 41—“ANY ACT OR THING”

#### CASE #1: Allegations of Improper Conduct

The complainant alleged that CSIS had improperly used its resources to assist a former employee. Specifically, the complaint alleged that the Service had improperly collected information, disclosed information to a third party in violation of CSIS policy, deliberately misled a court proceeding and attempted to intimidate the complainant.

The Committee determined that there was no foundation to any of the complainant’s allegations of wrongdoing by the Service. The Committee made two recommendations for modifying CSIS policy designed to avoid circumstances in the future that might lead to similar such complaints.

#### CASE #2: Allegations of Improper Conduct and Violation of Privacy

The complainant alleged that in receiving and retaining without consent items of personal property belonging to the complainant, the Service acted beyond its authority, without just cause and in violation of the complainant’s privacy rights.

### 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.

In addition, under section 41(2) of the Act, the Committee cannot investigate a complaint that can otherwise be channelled through existing grievance procedures of the *CSIS Act* or the *Public Service Staff Relations Act*.

The Committee learned that during an investigation the Service had recovered certain items belonging to the complainant. Without informing the complainant, the Service retained possession of the items for several days before returning them to the owner. The Committee found that the complainant's contention that CSIS had acted inappropriately and outside the normal functions of its duties was justified. The Service acknowledged to the Committee that the recovery and return of the complainant's property could have been handled in a manner more sensitive to the complainant's concerns and needs.

The Committee recommended that the Service address the lack of policy guidelines regarding the retention of personal items that come into its possession. The Service has since acted on the recommendation.

### **CASE #3: Allegations of an Improper Investigation of Lawful Advocacy, Protest and Dissent**

The complainant alleged that the Service was illegally and improperly investigating a group of persons involved in lawful advocacy, protest and dissent. The complainant requested that the Service make public any evidence in its possession suggesting the involvement by this and other like-minded organizations in activities posing a threat to the security of Canada.

In correspondence with the complainant prior to the filing of the complaint, CSIS stated that it did not make a practice of investigating lawful advocacy, protest and dissent. The Service declined to confirm or deny the existence of an investigation of the group in question. As a general rule, CSIS neither confirms nor denies the existence of any particular investigation.

The Committee found no evidence that the Service was involved in the activities alleged by the complainant.

## **SECTION 42—DENIAL OF SECURITY CLEARANCE**

### **CASE #1: Denial of Security Clearance Based on Loyalty**

The complainant, an employee of a federal institution, was denied a level 2 (Secret) security clearance. As a result, the complainant's employment with the federal institution was terminated. The Deputy Head of the federal institution based the decision to deny the complainant's security clearance on advice received from CSIS. The employee elected to contest the denial of clearance by filing a complaint under section 42 of the *CSIS Act*.

In its investigation, the Committee learned that the Service's advice was based on its assessment that the complainant was engaged in activities that constituted threats to the security of Canada and that the complainant associated with persons or groups regarded as security threats. The Committee found the Service's information to be credible and that the decision of the Deputy Head to deny the security clearance met the standard of "reasonable grounds to believe" as required by Government Security Policy.

The case raised two subsidiary issues for the Committee. Some CSIS investigators employed a certain format for preparing interview reports. The Committee recommended that this particular format be revised or abandoned. The Committee also reiterated its view (*see SIRC Report 1999–2000*, p. 73) that CSIS could mitigate the potential for conflicting accounts of security clearance interviews either by recording them and retaining the tapes on file, or by preparing an interview summary for the interviewee's comment and signature.

#### **CASE #2: Denial of Security Clearance Based on Loyalty**

The complainant was a former employee of a federal institution whose application for a level 2 (Secret) security clearance was denied. As a result, the complainant's

### **Complaints About Denial of Security Clearances 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 with SIRC 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)*

employment with the federal institution was terminated at which time the complainant contested the denial via a complaint to the Committee under section 42 of the *CSIS Act*.

Following a review of the evidence gathered by the Service to justify its advice to deny a security clearance, the Committee agreed that the complainant's loyalty to Canada was extremely doubtful. The Committee recommended that the decision of the Deputy Head of the federal institution to deny the clearance based on this advice be upheld.

## CANADIAN HUMAN RIGHTS COMMISSION REFERRALS

### CASE #1: Allegations of Discrimination Based on Gender and Ethnic Origin

The case was a referral from the CHRC of a discrimination complaint by a group of 12 current and former employees of CSIS. The complainants alleged that they had been subject to discrimination by their employer because of their gender and their ethnic origin.

The complainants asserted that their exclusion from positions that paid a higher salary for similar work amounted to gender and ethnic discrimination. For its part, the Service maintained that the higher-paying positions required a particular skill that the complainants did not possess.

With respect to the complaint of sexual discrimination, the Committee found that the complainants had failed to make a *prima facie* case that CSIS had discriminated against them based on gender. With respect to the complaint of ethnic discrimination, the Committee found that here too, the complainants had failed to make a *prima facie* case.

Based on the evidence presented to it, the Committee concluded that the salary bonus afforded to those employees with the requisite particular skill was based on a *bona fide* occupational requirement, and that there was no discrimination by the employer. The Committee provided the CHRC with its report. The CHRC will render a decision on the matter.

### CASE #2: Allegations of Discrimination Based on Ethnic Origin

The complaint alleged that because the complainant was a member of an ethnic minority, CSIS had treated the individual in an adverse and discriminatory manner and, through its actions, caused damage and prejudice to the complainant's

personal and professional life. The complainant maintained that the Service had conducted surveillance; had interrogated employers, colleagues and friends; and had caused the complainant to lose employment on several occasions.

From its investigation, the Committee determined that the Service had in fact contacted a former employer as well as an acquaintance of the complainant in an effort to locate the individual for an interview. However, the Committee saw no evidence that these contacts were the result of discrimination of any kind. Nor could the Committee find any evidence that these contacts resulted in prejudice to the complainant's employment status. The Committee concluded that the allegations of discrimination were without foundation. The Committee provided the CHRC with its report. The CHRC will render a decision on the matter.

## Section 3

---

### Accountability Mechanisms









































































