

## 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

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

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

and their supporting documents, operational reports, human source logs, internal CSIS correspondence and records of exchanges of information with other agencies and departments.

#### 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

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

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

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.**