Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1996-1997

Titled "Case Studies" in past reports, this part of the audit report presents the results of major research and analysis carried out by the Committee in the course of the year. As the new title implies, these inquiries are in addition to, and are intended to complement and reinforce, the other forms of audit research the Committee undertakes.

The Committee's selection of topics to be the subject of in-depth inquiry (this year there are five) is influenced by a number of factors including *inter alia*, shifts in the nature of the international threat environment, changes in technology, the need to monitor or follow up on past Committee recommendations, significant alterations in Government policy which the Committee believes could have implications for Service activities, changes in organizational structure or operational emphasis within the Service itself, and the interests of individual Committee Members.

This year, the subjects of the Committee's special interest are CSIS activities in the investigations of emerging threats, the Service's foreign liaison program, the means by which the Service manages human sources, CSIS efforts in addressing economic espionage, and the Service's activities concerning a particular homeland conflict.

Investigations of Emerging Threats

Since the end of the Cold War, many states and intelligence services of former foes have undergone a major transition. We reviewed how CSIS investigated the new and emerging threats to Canada's national security posed by the intelligence agencies of these states.

The Service's investigations of these threats were launched at the beginning of the decade. CSIS obtained information from foreign intelligence agencies and interviewed Canadians with a knowledge of developments in the states concerned.

After several years of monitoring the situation, CSIS terminated most of the targeting authorizations against the foreign states, owing to the absence of evidence that they were conducting intelligence activities against Canada. The Service retained, however, a general authorization to cover new threats which might arise. We concluded that the CSIS investigations were entirely appropriate, given the rapidly changing political environment at the time.

Below, we present our conclusions about certain of CSIS activities in this area. In most of the investigations that we examined, the Service's actions were prudent.

We concluded that the CSIS investigations were entirely appropriate, given the rapidly changing political environment at the time

In one case, however, we saw contradictory information about the seriousness of the threat and the Service's actions appeared to be excessive.

A foreign intelligence service investigation of note

In the case of one foreign state, CSIS conducted an extensive investigation. The Service believed that the foreign intelligence services continued to target ethnic Canadians at home and abroad. Furthermore, a foreign agency clandestinely collected information in Canada, some of which was economic, and attempted to sway Canadian government policies.

. . . foreign intelligence services were attempting to reactivate sources in Canada . . .

The Committee examined the Requests for Targeting Authority for this investigation.[2]

The Requests hypothesized that the new intelligence services were:

- establishing intelligence missions abroad, including Canada;
- continuing the predecessor agencies' practice of attempting to manipulate ethnic communities; and
- "...engaged in intelligence collection activities including the targeting of Canadians in Canada and abroad."

In addition, we examined the documentation that described how the new intelligence services were continuing the practices of their predecessors.

In our view, the evidence of these activities was equivocal. For example, we observed that CSIS seemed to place a negative interpretation on one activity which taken in context seemed to us to be relatively benign. We found that the reports CSIS provided to consumers in other parts of the government suggested that most of the alleged intelligence activities were innocuous. Finally, we took note of the fact that an intelligence service allied to Canada decided not to pursue investigations of the foreign intelligence services in question.

The Committee did encounter some evidence that the foreign intelligence services were attempting to reactivate sources in Canada used by the previous regime. The Service's focus, however, was not so much on the current activities of the foreign services, but rather on their preparations for future intelligence activities.

Other emerging threat investigations of note

We noted several issues of concern in the other investigations that we reviewed:

- A CSIS official pressed a foreign diplomat posted in Canada for information although the diplomat, who was suspected of being a foreign intelligence asset, had clearly changed his mind about speaking with the Service. To the Committee, the officer's persistence was questionable in the circumstances.
- CSIS officers placed into the Service's computer banks extensive accounts about the internal politics of some states. The information was received by CSIS on an unsolicited basis.

2. For more information about targeting authority, see inset on page 17.

- CSIS investigators repeatedly questioned one target. To us, the questioning appeared confrontational and out of proportion to the threat he posed.

- The Service provided adverse information about a person to two Federal Government departments and to an allied intelligence agency. We noted that the Service described the target as a "witting agent" of a foreign intelligence service, a potentially damaging statement not substantiated by the documentary evidence we saw. In addition, the authority to investigate him was not properly approved; it did not take into account his immigration status, as required by policy. CSIS later rectified the error.

CSIS Liaison Program with Foreign Agencies

SIRC's reviews of the Service's foreign liaison activities were conducted pursuant to section 38(a)(iii) of the *CSIS Act*.[3] We reviewed the foreign liaison program in general, and the exchanges of information with foreign agencies at nine posts abroad in particular. The audits focused on the accountability procedures and controls in place, and examined whether CSIS had placed restrictions on the dissemination of certain types of information to foreign agencies. We also inquired into CSIS relations with foreign agencies as carried out by its Security Liaison Officers (SLOs) as well as the SLOs' relations with Canadian Federal officials.

The reviews had several objectives:

- to ascertain the status of several issues that repeatedly arose in past reviews;

- to ensure that there was no excessive or unnecessary use of powers by the Service;

- to review the effectiveness of the Service's tracking systems for information exchanges; and

- to learn if there were systemic problems that impacted on the Service's foreign liaison program that had not already been identified.

Methodology of the current review

The Service operates Security Liaison Officer (SLO) posts overseas responsible for liaising with police, security and intelligence agencies in a large number of countries. The authorities in the host countries concerned are aware of the Service's officers presence and functions, a necessary pre-condition for inter-agency cooperation.

In fiscal years 1995-96 and 1996-97, SIRC undertook a series of reviews of the CSIS SLO posts abroad. We conducted these audits as a result of our review of the documentation from one post in 1994-95.[4] That study sought to audit the exchanges of information with other agencies conducted through the post solely from the documents available at CSIS Headquarters. The findings prompted concern that the numerous problems we found might be systemic in nature. We then undertook to review additional SLO posts.

. . . The audits focused on the accountability procedures and controls in place

3. "...to review arrangements entered into by the Service pursuant to subsections 13(2) and (3) and 17(1) [mandating CSIS to enter into arrangements with foreign powers, agencies and international organizations] and to monitor the provision of information and intelligence pursuant to those arrangements."

4. SIRC *Annual Report* 1994-95, Chapter 4(ii), page 28.

The major focus of the reviews was to examine the documentation retained at CSIS Headquarters for nine SLO posts. On-site reviews at three of these posts were conducted to ascertain whether the material sampled at CSIS Headquarters from the same posts was representative of the information provided by the Service to foreign agencies. In addition, at CSIS Headquarters we examined the correspondence from six other posts. For purposes of comparison, we audited the information disclosures to foreign agencies for the same period of time.

To supplement this information, we interviewed Service staff at CSIS Headquarters and at selected posts, and we examined open information from other sources (human rights groups, for example). In addition, we conducted a special audit of "direct exchanges" — information that CSIS provides to foreign agencies via telecommunications circuits — in order to determine if important information was bypassing the controls associated with the SLO posts.

Information exchanges with foreign agencies were examined with the following questions in mind:

- did they conform to the statutory guidelines for the retention, dissemination or receipt of the information?
- were they in conformity with the arrangements Canada entered into with the agency in question?
- was the information provided by CSIS to the foreign agency accurate and was the potential for damage to the person weighed against the importance of the investigation?

Background to the Service's Foreign Liaison Program

From the inception of CSIS in July 1984, until 1989, CSIS had a Foreign Liaison Branch. In 1990, the Service replaced the Branch with a new system for communicating with and coordinating the efforts of the SLOs. At the time, SIRC expressed its concern about the disbanding of the Foreign Liaison Branch. The Committee regretted the loss of what it described as "An intermediary... [that could] 'blow the whistle' on the inappropriate dissemination of information abroad."[5]

In its place, CSIS created a new unit under a Coordinator, to provide administration and support services to the SLOs. The Coordinator reported to one CSIS executive member, while the SLOs reported directly to another. The Foreign Liaison Advisors reported to their respective operational branches, and were to monitor the correspondence exchanges and ensure that the SLOs were informed about new developments.

In a previous Annual Report,[6] we expressed concern about the number of SLO posts CSIS was closing and were of the opinion that, "the foreign liaison program would benefit from more attention from the Service, not less, as seems to be the trend in terms of representation overseas."

For a number of years, there were few changes to the Service's posts abroad, save for the post closings, but the mid-1990s saw a major reworking of the Service's foreign liaison strategy. Decisions to open as well as close selected Security Liaison Officer posts resulted, as did changes to the management structure of the foreign liaison program as a whole.

In 1994-95, the reporting relationships and responsibilities changed for both the unit and the SLOs, as a result of an internal management study. Most notably, the overall management of the program was once again centralized under the direction of a senior manager. We understand that in 1997, to a certain extent, history will repeat itself. The foreign liaison program will be raised to Branch level once again, an initiative the Committee will report on in our next Annual Report.

5. A SIRC Review of CSIS' SLO Posts (London & Paris), 12 January 1993.

6. SIRC *1993-94 Annual Report*, page 26.

- were the control provisions, including recording methods, for the information provided by CSIS properly observed?

Results of the review: CSIS' organizational initiatives

In 1995, the first meeting of a new CSIS committee took place, the establishment of which arose from an internal CSIS program review. Chaired by the Chief of the foreign liaison program, the committee was established to serve as a coordinating and information sharing body between CSIS Headquarters' branches and the overseas posts. The purpose was also to provide strategic direction for the management of the Service's foreign liaison program. We believe the initiative is a positive one.

As well, the Committee regards the re-establishment of a Foreign Liaison Branch as a constructive decision. With the increasing interdependence of the global intelligence community, the liaison responsibilities of the foreign liaison program will also expand and a branch-level infrastructure will likely help the Service manage the increasing work load.

In previous SLO post reviews, we have commented on the adequacy of the Service's Procedures Manual for SLOs. In 1993, the Field and Liaison Unit at CSIS Headquarters published a Foreign Liaison Procedures Manual to replace an outdated manual. The new manual deals primarily with administrative matters and instructs SLOs to maintain a log of all incoming and outgoing correspondence on a specific form.

We noted that because of the relative isolation of the SLOs from CSIS Headquarters, the existence of a document containing basic procedures to assist them is more important than it would be for Canada-based CSIS staff. We observed that whereas in the 1980s, the Service provided the SLOs with a rather comprehensive body of instruction specifically for the posts, the "new" Procedures Manual is already out of date and contains only information on routine administrative procedures.

> We recommend, therefore, that the Procedures Manual be brought up to date, and that it cover important post issues that are not addressed elsewhere.

The Service informed us that it concurs with the need to update the Procedures Manual on a priority basis.

In the course of the Committee's liaison post audits, we learned that the Chief of the foreign liaison program had conducted a management review of one SLO Post, and intended to conduct others where warranted. We regard this as a sensible initiative.

Results of the review: CSIS foreign communications tracking procedures

The Service's foreign liaison program must be able to respond to information demands from within the Service, as well as from domestic and foreign agencies. However, the Committee has in the past been critical of the Service about its unreliable system for

The Committee regards the re-establishment of a Foreign Liaison Branch as a constructive decision

tracking the information it provides to foreign agencies. This problem, as well as others that arose due to communications deficiencies the Committee identified within the Service, were unresolved.

The Committee has in the past been critical of the Service about its unreliable system for tracking the information it provides to foreign agencies

Logging and data tracking

In 1985, CSIS developed a form it said was intended "to assist SIRC in its duty under section 38(a)(iii) to 'monitor the provision of information and intelligence pursuant to ... arrangements.'"

The written log that the Service implemented at that time was complicated and difficult to interpret, so in subsequent years, CSIS Headquarters sent out memoranda and telexes to help SLOs understand how to complete the form.

During the course of our SLO reviews, we repeatedly attempted to use the logs of information exchanges with foreign agencies created by SLO posts (and held at CSIS Headquarters). These attempts were thwarted by the difficulty in locating the documents at Headquarters referred to in the logs compiled at the posts. The only reliable way to find and examine the documents listed was to visit the SLO post itself.

In recent years, the Service introduced an electronic tracking system. SIRC staff have since attempted to check the data in the new system against the information in the logs so as to ensure that the audit samples were representative of the messages sent abroad. Our current audits establish conclusively that it is not possible to correlate the log and electronic tracking systems. In commenting on these difficulties, the Service informed SIRC that "at least part of the problem is that the post logs contain more than just section 12 [intelligence] information. Cooperation and administration tasks are also recorded."

Linked to this problem was a deficiency the Committee found in the Service's system for reporting reliable statistics on the volume of information exchanges carried out by Security Liaison Officers.

Subsequently, and at the invitation of the Service, SIRC identified problems perceived to exist within the Service's information recording and reporting system. Thus, beginning in late 1996, the Service implemented a new automated system for use at SLO Posts. The system is designed to streamline reporting procedures and address SIRC accountability requirements.

We appreciate the fact that the Committee's input was requested and, at first glance, it appears that the Service has attempted to address our concerns in this area. Future audits will test the success of the new system.

Distinctions between exchanges of "open" and "classified" information

One of the recurring issues for SIRC in its review of CSIS information exchanges with foreign agencies, is the extent to which SLOs can provide open information to foreign agencies. We observed that the Service's *Operational Policy Manual* makes no distinction between the treatment to be afforded open and classified information.

CSIS has made a distinction, however, between open information collected as part of a section 12 investigation, for example, and open information to which SLOs have access, but is not collected or retained as part of the "corporate record."

For open information that is collected as part of an investigation, the Service's position is that the same rules governing the disclosure of classified information to foreign agencies apply to open information collected and held on Service files under a section 12-mandated investigation. Open information which comes to the attention of SLOs via other means, however, such as newspapers, magazines, and the like, may be passed at the SLO's discretion providing it meets the Service's criteria for what is appropriate.

We were concerned about the impact of adverse open information that SLOs can release to foreign agencies. We noted one case where the provision of open information to a foreign agency triggered a foreign agency investigation.

The Committee has noted the efforts of the foreign liaison program to deal with our concerns regarding the provision of open information to foreign agencies. We consider it a positive move that the unit has attempted to achieve an understanding in this area.

> We recommend, however, that when an SLO decides to disclose adverse open information about Canadians to a foreign agency, the SLO be required to first consult with management at CSIS Headquarters.

Information exchanges not passing through SLO posts

Our reviews of "direct (telecommunications) exchanges" described the importance of direct links between the Service and several allies for Canadian security interests. For the period under review, we found that the SLOs were always notified when a direct exchange occurred; that all CSIS requests or responses were made under a valid authorization; and that the exchanges were captured in the Service's electronic tracking system. We were satisfied with the Service's use of the telecommunications links.

Results of the review: CSIS assessments of other agencies

Each year, SLOs provide CSIS Headquarters with assessments of the foreign agencies that cooperate with the Service for the purpose of aiding the operational branches to decide what should and should not be disseminated to these agencies. With the introduction of SLO ratings several years ago, SIRC had welcomed the Service's initiative because it held out the prospect for better informing CSIS operational staff about the various factors that might influence decisions about such dissemination. Recent audits have given the Committee reason to reconsider its initial enthusiasm.

As noted above, the current series of SLO audits was prompted by an earlier SIRC evaluation where we saw that agency assessments were

We were concerned about the impact of adverse open information that SLOs can release to foreign agencies

of uneven quality and that the human rights situations in several countries were not adequately described. CSIS maintains that human rights considerations are taken into account.

For this latest series of reviews, we conducted an on-site audit at the same post that prompted the broader SLO review. We found that despite poor human rights situations and political instability generally in many of the countries in the region covered by the post – in addition to high levels of corruption in some cooperating agencies – these organizations continued to receive favourable SLO ratings.

Some SLO agency assessments did not contain information on human rights

Our survey of the foreign agency ratings procedures identified specific concerns:

Attributing the information source
The ratings are set by the SLOs on the basis of the information collected *en post*. The assessments represent the perceptions of the SLOs based upon their day-to-day dealings with the foreign agencies, what they read in the media and elsewhere, and information shared with SLOs by other staff at Canada's missions abroad.

It is the Committee's view that where the reliability ratings reflect the experience of other Government of Canada sources available to the SLO — Foreign Affairs or Immigration department staff, for example — and in the absence of sufficient information held by the SLO itself, agency assessments should attribute the ratings to the other parties.

Definitions of reliability
We believe the current operational definitions employed in the reliability ratings system are ambiguous and thus open to a level of individual interpretation that reduces the system's effectiveness as an operational tool. With the emergence of the new democracies and with the expanding number of foreign arrangements, the need for a well-defined system of rating the reliability of the foreign agencies is essential.

> We recommend that the Service revise, or at least better define, its system of evaluating the reliability of foreign agencies.

Agency assessments and human rights concerns
According to Ministerial Direction, CSIS must consider the human rights conditions in those countries with which it is considering sharing information. Our recent reviews have found, however, that some SLO agency assessments did not contain information on the human rights situations for countries where we would consider the discussion warranted.

Earlier SIRC audits in the current series indicated that references to human rights in assessments were only sporadic, notwithstanding the fact that human rights is an issue SLOs are obliged to comment on. In the aftermath of our earlier reports, agency assessments we saw did document the human rights situation in a number of countries, but there is room for improvement still. Current audits identified a number of assessments which failed to provide current information on recent important events and others that have not been updated for several years.

The Committee regards CSIS' agency assessment process as an opportunity that has yet to be fully exploited. We believe that this problem can be remedied by the Service, as evidenced by some of the most recent assessments.

Defining types of liaison

A principal Ministerial Direction to the Service sets out the various types and levels of liaison Canada has with foreign agencies. Cooperation with other agencies can range from routine immigration vetting all the way to personnel exchanges. In a number of SIRC studies conducted in the series examining foreign agency cooperation, we found that the decision as to which sort of activity falls under what liaison arrangement is subject to varying interpretation.

SIRC identified one exchange with a foreign agency which we considered to be inappropriate in light of existing Direction. CSIS had never asked the Solicitor General to approve this type of exchange with this particular foreign agency. CSIS did not agree with our interpretation, maintaining that the type of assistance rendered was in accordance with an existing, Minister-approved arrangement.

We also observed that the Service's definitions for the scope of arrangements appear in neither Ministerial Direction nor in CSIS policy documents. The Committee would like to see the Service provide clear definitions for the various exchange arrangements it manages.

On the policy front, a Ministerial Direction that pre-dates CSIS has outlived its usefulness in a number of areas. We hope that a new Ministerial Direction forthcoming will remove the ambiguity as regards the definitions of foreign arrangements.

Logging of oral directions and information exchanges

In two past reviews, we have noted that SLOs or staff at CSIS Headquarters sometimes failed to log certain kinds of oral exchanges, specifically conversations with persons in foreign agencies and important instructions relayed to the SLO by CSIS Headquarters personnel. We were also concerned about a statement to us by one SLO that there was no policy direction requiring that such oral exchanges be logged. The CSIS *Operational Policy Manual* clearly states otherwise. The Service notes that these incidents were isolated cases.

For the purpose of accountability, we believe that all meetings with foreign agencies where operational information is exchanged, whether orally or in writing, should be documented. All CSIS Headquarters personnel should document the instructions they provide to SLOs, regardless of the means of communication. The Committee is also of the view that Headquarters branches should remind staff of the existing requirement to document operational instructions conveyed orally to SLOs.

Our disagreement with CSIS in this area appears to focus on whether operational information has or has not been recorded. We have found some examples of where this was

The Committee would like to see the Service provide clear definitions for the various exchange arrangements it manages

unequivocally the case. We expect to find more in the future if the Service does not reiterate the existing policy to its employees in the ways suggested above.

Altering or transferring existing liaison arrangements

A long-standing Ministerial Direction requires CSIS to obtain the Minister's approval to establish a liaison arrangement or alter the scope of an existing one. However, SIRC found cases where the Service transferred agreements from one agency to another in the absence of Ministerial approval. CSIS had instead sought and obtained authorization from senior officials in the Ministry of the Solicitor General.

Where the transfer takes place because an agency undergoes a name change or has received expanded responsibilities, we do not object. Sometimes, however, the proposal is to transfer existing arrangements to a new agency with its own new mandate and personnel. We believe that Ministerial approval, not just that of Ministry officials, is necessary to comply with the Direction when a liaison arrangement is to be transferred to another agency, regardless of whether the scope has changed.

Management of Human Sources

Human sources function at the direction of CSIS to collect and provide information to the Service. The rules which govern their management stem from Ministerial Direction and written CSIS policies. Following the events involving the Heritage Front in 1994, the Direction and the concomitant policies were amended. In the period following the dissemination of the new directions, the Committee wanted to see if the revisions to the rules had resolved the concerns we set out in our special report to the Solicitor General — *The Heritage Front Affair*.

CSIS Management of Human Sources and the Heritage Front Affair

In *The Heritage Front Affair*, the Committee wrote that a CSIS source was involved in a harassment campaign[7] by white supremacists. The senior Service managers said that they had not been apprised of this activity, nor did they sanction it. The Committee concluded that CSIS policy and direction in the source management area was "seriously deficient."[8] SIRC accepted that sources could not merely be passive. The Committee said, however, that CSIS officials "should regularly stand back from day-to-day transactions to assess the operation in its totality;" that is, they should draw up a "balance sheet" of the benefits and dangers of a particular operation. While the Committee did not "advocate detailed rules that would unduly limit CSIS," we did conclude the following:

> We recommend, rather, Ministerial guidelines that require CSIS management to carefully weigh the benefits and the dangers of each human source operation on a regular basis; taking due account of the special circumstances of each case.[9]

On 1 August 1995, the Solicitor General issued a new Ministerial Direction to the Director of CSIS on human source use in response to the issues raised by the Committee in *The Heritage Front Affair*. The Ministerial Direction, and the subsequent policy changes expanded the controls on sources in three areas: *agent provocateur* activities, discreditable conduct activities, and activities touching upon sensitive institutions such as campuses, religious institutions or trade unions.

7. SIRC Report. *The Heritage Front Affair*, Report to the Solicitor General of Canada, Section 5, 9 December 1994, pp. 9-10.

8. *The Heritage Front Affair*, Section 13, p. 12.

9. *The Heritage Front Affair*, Section 13, p. 14.

We sought to examine all source operations that could influence targeted or non-targeted organizations or groups. We also sought out cases that involved *agent provocateurs* or disreputable conduct, and here we found no new ones. But we identified a number of cases where sources were involved with sensitive institutions; of these we audited several.

We concluded that the majority of the cases reviewed were in compliance with the revised Ministerial Direction and written policy. We believe that the operations were reasonable in terms of the intelligence they yielded: in a number of cases the potential for serious violence was very likely averted because of the information gained. Several operations involved considerable danger to the country had they not succeeded since the acquisition of weapons and explosives was at issue. In sum, SIRC believes the operations were justified and concludes that CSIS officials demonstrated adequate control over the actions of the sources.

We found problems in three cases:
The first operation involved a source who reported on a meeting that occurred in the course of collecting information about a target. CSIS managers told the source that they had no interest in the milieu where the meeting occurred, a context which involved legitimate dissent and protest. The Service's records, however, contain a detailed account of a meeting attended by the CSIS targets. Much of the reporting involved statements that stopped short of suggesting violence by persons who were not targets. In addition, the Service obtained information about an imminent, non-violent demonstration, and subsequently disseminated the information to the police.

The second case involved a CSIS operation that, in the view of the Committee, posed a potential risk to a sensitive institution – namely, the free flow of ideas on a university campus. Intelligence suggested that there was a potential threat, and CSIS was of the opinion that the threat warranted the risk. The Service terminated the investigation.

The third case gave rise to questions concerning the origin of certain information CSIS collected. The source was a government official who in the normal course of work had access to sensitive personal information. The Service was interested in the source's knowledge about a particular community, not in information the source might have gained through work. CSIS managers did not, in our opinion, adequately document their instructions that the source was not to provide information acquired in this manner. When SIRC researchers came across information that appeared to come from the source's occupation, inquiries of the Service were made. We subsequently ascertained that the information was not improperly acquired.

SIRC will continue to monitor the Service's management of human sources.

We sought to examine all source operations that could influence targeted or non-targeted organizations or groups

Economic Espionage

At the time we last commented on CSIS' economic security effort in 1993, the program was new, and the state of knowledge about economic

espionage was limited. The program is now six years old and the Committee's review indicates that the main difficulty confronting the Service in this area is its own overly broad definition of what constitutes an economic threat.

The Service faces considerable obstacles to reasonably defining its role in dealing with economic threats to Canada. Economic espionage can target many sectors of Canada's economy, and the threats can emanate from foreign governments, agencies or individuals working on their behalf. It is often very difficult to differentiate between the activities of private sector companies and those of governments.[10] Nonetheless, a reassessment of the Service's definition of what constitutes an economic threat and how that definition is applied in its operations, is warranted.

What is an "economic threat"?

When we examined the Service's economic security investigations it was evident that CSIS' definition of economic security — which includes "information of economic significance" — transcends those

Background to CSIS Economic Security Program

The changing international threat environment of the post-Cold War world has pushed economics to the top of the national intelligence agendas of many countries, Canada not excluded. The Government of Canada has broadened its definition of national security to include the concept of "economic security" which CSIS defines as "the [set of] conditions necessary to sustain a competitive international position, provide productive employment, and contain inflation."

Reflecting these changes in the nature of the challenges to Canadian security, the Service initiated in June 1991 a comprehensive approach to two issues: "Economic Security" and the "Proliferation of Weapons of Mass Destruction." In order to coordinate the existing organizational sections within CSIS investigating these areas, the Service formed the Requirements Technology Transfer (RTT) Unit.

Economic Security and Proliferation Issues (ESPI) Unit
In October 1995, the Service restructured the RTT unit into what is now the Economic Security and Proliferation Issues (ESPI) Unit. ESPI's economic security mandate is to investigate "the clandestine acquisition or transfer, by foreign governments, of proprietary/classified technology and information valuable to Canada's economic interests."

Liaison/Awareness Program
One of ESPI's primary means of carrying out its responsibilities is through the Liaison/Awareness Program. Under this program, ESPI meets with members of the business, government, academic, and scientific sectors in order to raise their awareness about economic security. The Liaison/Awareness Program and the ESPI investigations relating to economic security are carried out under a targeting authority from the CSIS Target Approval and Review Committee (TARC).

Targeting Authority
The targeting authority sets out the criteria as to what can be investigated as an "incident of economic espionage" under the Service's mandate. An incident must involve: the participation of a foreign government, activities of a clandestine or deceptive nature, the potential acquisition of proprietary/classified information or technology, and be detrimental to Canada's economic security.

10. The Service notes that foreign states are not inclined to advertise their involvement in the clandestine procurement of economic intelligence. CSIS investigates to ascertain whether incidents are economic or industrial espionage, the latter being the responsibility of the private sector.

technological developments many people would regard as vital to Canada's economic security. Under the service's definition, such information can range from economic policy to supplier lists. In the cases we reviewed, we were hard put to see a strong link between a foreign government and the loss of certain types of economic information, such as client/supplier lists. The Service states that such a loss is considered economic espionage if a foreign state sponsored or facilitated the loss.

An analysis of the information gathered by the Service leads us to conclude that the Service collects and retains information not specifically linked to threats to the security of Canada. While the Service has developed adequate criteria to target particular incidents of economic espionage, we found that the Economic Security and Proliferation Issues (ESPI) unit investigated some incidents which did not appear to meet those criteria.

For example, ESPI investigated several incidents that, we believe, did not have a demonstrable link to a foreign government, including activities that were primarily of a criminal nature.[11]

We also observed that CSIS sometimes collected information from briefings and presentations under the Liaison/Awareness program that was often administrative, and not specifically linked to threats to the security of Canada.

> We recommend that adminis- trative information collected from the Liaison/ Awareness Program be retained in a non-section 12 data base.

We wish once again to reiterate the view we expressed in our 1993 review, that CSIS has a role to protect those areas of Canadian technology which bear directly upon national security, and about which it is necessary to advise the government. The Service should investigate only those activities that constitute "threats to the security of Canada" as set out in its mandate.

Intra-government cooperation

Since our most recent review of the economic espionage investigations revealed relatively little cooperation and coordination between CSIS and other government departments, a forthcoming SIRC study will look specifically at these issues. The investigation of economic espionage requires that the Service have access to, and make efforts to employ, both technical and business-related expertise.

The Service faces considerable obstacles to reasonably defining its role in dealing with economic threats to Canada

A Homeland Conflict

The Committee reviewed the CSIS investigation of some persons in Canada who were associated with an internal armed conflict in an overseas country. The review covered the period from April 1994 through March 1996, and was a follow-up to a previous Committee review of similar activities in the period 1990 to 1992.[12] The CSIS investigation concentrated on the activities of a small number of people who supported the conflict

11. The Service maintains that under section 2(b), it can conduct preliminary inquiries to corroborate a foreign intelligence lead on the possibility of criminality, before advising the police. We will judge these matters on a case by case basis.

12. SIRC *Annual Report 1992-1993*, page 22.

through a variety of activities on behalf of organizations that were parties to it.

The 1996 CSIS *Public Report* refers to activities that have been used to support terrorist actions, including fundraising, advocacy and information dissemination. These types of activities could, consequently, be of legitimate interest to the Service under section 2(c) of the *CSIS Act*.

Accordingly, our audit set out to determine whether the activities that CSIS investigated indeed represented a threat to the security of Canada, and whether the investigation complied with legislation, Ministerial Direction, and CSIS policy and procedures. We were also interested in whether the Service had followed up appropriately on concerns that we had expressed in the earlier review. To this end, we examined the Service's documents and, where appropriate, we sought clarification of questions arising from the document review.

Targeting decisions

After measuring requests from CSIS officers to senior management for targeting approval against the Service's established policies, and seeing whether the documents we examined substantiated the requests, we have determined that CSIS had sufficient grounds to conduct the investigation and employ the investigative methods authorized by senior management.

To receive targeting approval, CSIS policy calls for a complete and balanced description of the activities of the targets. SIRC researchers found that one of the requests could have been more complete and better balanced. For example, a request submission expressed concern about the possibility of violence occurring in Canada, but did not include information in the Service's files to the effect that a party to the insurrection at issue was unlikely to change its practice of confining terrorist activity to the homeland. The Service asserts that the inclusion of this information would not have altered the decision to approve the investigation.

CSIS' Role in Preventing Politically Motivated Violence

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

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

Conduct of the investigation

Our review focused on a small number of persons who were targeted, human sources who reported on the targets under investigation, and other investigations conducted under the targeting authorizations. The individuals investigated were leading members of their respective organizations, and had been included in the earlier SIRC audit report. We agreed both with CSIS' decision to continue investigating the activities of these persons and with the means of investigation the Service employed.

Our researchers examined CSIS documentation to determine if the investigation was consistent with the authorization and see if the Service had reasonable grounds to suspect a threat to the security of Canada.

The targeting authority for the investigation was directed at groups in Canada which operated in support of the principal organization conducting the armed insurgency in the homeland. Since there are smaller, less significant groups involved in the struggle who may also have adherents or supporters in Canada, CSIS found it necessary to investigate the possible supporters of one such group and did so under the investigative authority assigned to the principal organization.

While the Committee is in accord with the Service's decision to investigate the smaller group, we believe it should have been carried out under an authority separately obtained.

The Committee found one instance where we believe the Service had insufficient grounds to carry out certain investigative measures against a person rumoured to be providing funds to an insurgent group in the homeland.

In a previous SIRC audit report, we expressed our concern about a CSIS investigator who appeared to use a community interview in order to inappropriately obtain personal information from the subject being interviewed. In the course of the current review, we found that the Service conducted interviews in several cities across Canada to learn more about the ethnic communities and to assess the extent and nature of a possible threat. These interviews were conducted appropriately.

We randomly selected a small number of human sources for review. We were interested in the relevance and reliability of the information provided by these sources with respect to the activities under investigation, whether the management of the sources was consistent with law and policy, and whether there were any unusual problems.

While we found that, in general, CSIS' investigation was in accordance with its operational policy, and the information it collected was necessary for the investigation, we identified one inappropriate action. A source reported on the activities of targets by attending a meeting on a campus without obtaining the prior approval of the Solicitor General as is set out in Ministerial Direction. CSIS has acknowledged this to be a compliance issue and is investigating.

CSIS had sufficient grounds to conduct the investigation and employ the investigative methods authorized by senior management

We found the exchanges with foreign agencies were consistent with the agreements in force

Liaison and exchanges of information with foreign agencies

In its 1993 report, the Committee drew attention to a case where CSIS inappropriately provided information to a foreign agency about the travel plans of a Canadian resident to a country with a poor human rights record. The most recent review shows no incidents that would raise similar concerns.

In all of the cases we reviewed, we found the exchanges with foreign agencies were consistent with the agreements in force.[13]

Quality of advice to government under section 12[14]

CSIS discloses the information it has collected to government clients in formal written reports and briefings. An issue for our review was whether these reports accurately reflected the information in the Service's files. We concluded that CSIS reports to Government on this investigation — while tending to be general in nature — were useful and timely.

Section 15 immigration security assessments[15]

The aim of this review was to assess the appropriateness of CSIS actions with respect to the powers it exercises under section 15 of the *CSIS Act* in connection with individuals from the same country whose conflict was the subject of the broader CSIS investigation.

SIRC wanted to ascertain whether the information in the briefs CSIS prepared on prospective immigrants was consistent with the information in the Service's operational and screening files, whether the Service's recommendations were consistent with this information, and whether the assessments were prepared in accordance with the Service's operational policy. Five randomly selected security assessments prepared by CSIS were examined in depth.

The Committee was in accordance with the advice provided by CSIS in all of the assessments, and found a minor omission in one. It is evident that some information from a prospective immigrant/refugee's immigration screening interview was in fact entered into the section 12 data base. CSIS policy implies that the interviews of prospective immigrants are not to be used for other investigations. We believe that CSIS policy does not adequately address the collection of section 12 information during section 15 interviews. We have brought this issue to the Service's attention.

The Committee's general finding

The Committee has found that the Service's investigation in this matter was appropriate and that it was carried out in accordance with legislation, Ministerial Direction, and policy. We note also that following concerns expressed in SIRC's 1993 report, the Service adjusted its conduct of the investigation in a satisfactory manner.

13. For additional information on the CSIS Liaison Program with Foreign Agencies see page 3 of this report.

14. Section 12 of the *CSIS Act* mandates the Service to collect, analyse and retain information on threats to Canada and "report to and advise" the Government about what it has learned.

15. Under section 15 of the *CSIS Act*, the Service has the sole responsibility for security screening applicants for landed immigrant and refugee status.