B. Annual Audit of CSIS Activities in a Region of Canada

Report #111

Every year the Committee audits the entire range of CSIS investigative activities—targeting, special operations, warrants, community interviews, and sensitive operations—in a particular region of Canada. A comprehensive examination such as this provides insight into the various types of investigative tools the Service has at its disposal, and permits the Committee to assess how new Ministerial Direction and changes in CSIS policy are implemented by the operational sections of the Service.

The Targeting of Investigations

The targeting section of the regional audit focuses on the Service's principal duty—security intelligence investigations authorized under sections 2 and 12 of the *CSIS Act*. When examining any instance in which CSIS has embarked on an investigation, the Committee has three central concerns:

- did the Service have reasonable grounds to suspect a threat to the security of Canada?
- was the level of the investigation proportionate to the seriousness and imminence of the threat?
- did the Service collect only the information that was strictly necessary to advise the government on the threat?

Committee researchers also keep watch generally on the manner of the Service's adherence to its own internal operational policies, rules, and directives.

Methodology of the Audit

In the region at issue, the Committee selected eight investigations—six counter terrorism cases and two counter intelligence cases. Of the eight, three were issue-based investigations. SIRC researchers reviewed all files and operational messages in the Service's electronic

Management of Targeting

Target Approval and Review Committee
CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation
There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting
An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada, and are related to or emanate from that specific issue.

data base. Researchers also interviewed the CSIS officers who carried out the investigations as well as their managers.

Findings of the Committee
In all eight cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The targeting levels were proportionate to the seriousness and imminence of the threats in all but one case, and no actions were taken against non-targets. The Committee concluded that in all of the cases we reviewed, the Service collected only the information that was strictly necessary to advise the government about the threats.

In three instances, however, the Committee had reservations about the accuracy of some of the information presented to the Target Approval and Review Committee (TARC). We suggested to the Service that it take measures to enhance overall quality control of the information provided to TARC.

The cases which raised issues and concerns for the Committee are summarized below.

Targeting Level
The first case involved a counter terrorism investigation pertaining to a landed immigrant's involvement with a known terrorist group and his activities within an ethnic community in Canada. The person had been

under investigation for a number of years and during the period under review the Target Approval and Review Committee had authorized a higher level of investigation.

The Service's justification for requesting a higher level investigation was that it had information that the target's expertise was being sought by leaders of a known terrorist group, and that he had contacts with those leaders. However, our review showed that the Service had not collected information that in our opinion supported the more intrusive investigation. We believe that the original lower-level targeting authority was sufficient to address the threat posed.

The Regional Office used its investigative powers with parsimony and in proportion to the threats posed.

Termination of an Investigation

The second case involved a counter terrorism investigation of an individual in relation to the activities of a known terrorist group based abroad and with representatives in Canada. We agreed that the Service had reason to suspect the individual of activities that posed a threat to Canada. The target's behaviour lent credence to the Service's interpretation of the facts as presented to the Target Approval and Review Committee.

Our review showed that the Service's investigation revealed no pattern of terrorist activity, and that CSIS had quite properly terminated its investigation upon reaching that conclusion.

Accuracy of Facts Presented To The Target Approval and Review Committee

Case three concerned a counter terrorism investigation of an individual whose activities came to the attention of the Service as part of a wider investigation into a known terrorist group present in Canada. While we concurred with the Service's view that the target's relationship with known terrorist figures constituted a potential threat to Canada, we took issue with one part of its Request for Targeting Authority (RTA).

In a manner which bolstered the Service's case for the authority, the targeting request presented a fact that was not consistent with the information collected. When questioned by the Committee, the Service acknowledged the error. The Committee was of the view, however, that the discrepancy did not undermine the legitimacy of the targeting authorization.

Three Issue-Based Investigations

Cases four, five and six, were all issue-based investigations, two from counter terrorism and one from counter intelligence. In both counter terrorism investigations, the Committee found that CSIS had met the test of "reasonable grounds to suspect" in justifying its inquiries, that CSIS had collected only information that was strictly necessary and that there was no extensive reporting on individuals who were not already the subject of specific targeting authorizations. In sum, for these two cases, the Committee believes that the regional office used its investigative powers with parsimony and in proportion to the threats posed.

An Investigation of Economic Espionage

The Committee reviewed a case involving economic espionage. Investigations of economic espionage are conducted under section 2(a) of the *CSIS Act*, and Ministerial Direction notes that for the activities to warrant investigation they must be against

Canada (assets, policies or programs of the Government of Canada) or detrimental to the interests of Canada.

Since the Service's request for this investigation did not explicitly list Government assets or programs, its request fell under the "activities...detrimental to the interests of Canada" criterion. Ministerial Direction further specifies that in instances where it is unclear if the activities have a negative impact on the "national interests," the Service should seek guidance from another government department or agency.

Our examination of the information submitted to TARC in order to obtain a targeting authorization turned up an error of fact and two points we believe were overstatements in relation to intelligence reports on which the submission was based.

Obtaining and Implementing Federal Court Warrants

Under section 21 of the *CSIS Act*, only the Federal Court of Canada can grant CSIS the right to use warrant powers, such as telephone or mail intercepts. In requesting such powers, the Service must present an affidavit to the Court attesting to the facts which require their use. Every year, the Committee audits a number of affidavits by comparing them with information in the Service's files. In reviewing warrant affidavits, the Committee is focused on three central questions:

- do the facts presented in the affidavit accurately reflect the information used as the basis for its preparation;
- is the case that the Service presents to the Court set out in its proper context; and,
- are the facts, circumstances and statements of belief contained in the affidavit fully, fairly and objectively expressed?

1997-98 Developments Affecting the Warrant Process

As part of its audit, the Committee also reviews changes in Ministerial Direction and CSIS policy for the relevant period which govern the application for and implementation of warrant powers. We also examine all Court decisions that might impact upon the Service's use of warrant powers, as well as any significant changes to conditions accompanying the warrants.[12]

Only the Federal Court of Canada can grant CSIS the right to use warrant powers.

In 1997-98, there were no new Ministerial Directions or instructions pertaining to warrants. However, there were changes to CSIS policies and new Court decisions of interest.

Changes to CSIS Policies

As a result of restructuring at the Executive Level of CSIS, changes were made to the roles and responsibilities of certain officials in regard to warrant applications and the execution of warrant powers. The responsibilities include verifying that the warrant applications comply with Service legal and policy requirements, ensuring that the necessary resources are available to execute the warrants, checking that each application is processed on a timely basis, and approving all operations involving the powers granted by the Federal Court.

We also found that the Service amended its policies to tighten the controls in regard to intercepts of solicitor-client communications.

The Service has been employing greater precision and rigour in the preparation of its warrant applications.

New Court Decisions

Two Warrant Denials

In last year's report, the Committee commented on the Federal Court's denial of a small number of warrant applications. We reviewed these Federal Court decisions and found that the warrant applications were rejected because they did not meet the threat requirements of paragraphs 2(a) or 2(b) of the *CSIS Act*. We also learned that the Service later went back to the Federal Court with revised applications and the warrants were granted.

While the Committee did not identify any specific impacts of these decisions on the operational activities per se, we did observe that in accommodating the evolving judicial review process, the Service has been employing greater precision and rigour in the preparation of its warrant applications.

Changes to a Warrant Clause

In 1997-98, in what appeared to be another iteration of the McGillis decision,[13] the Federal Court removed the "reasonable grounds to believe" statement found in a certain clause. The amendment removed the discretion previously granted to senior Service officials in authorizing the execution of warrant powers against a certain type of target. The effect was to compel the Service to meet a higher threshold of certainty in the facts that it put before the Court. The Service subsequently deleted the particular statement from similar clauses found in all its warrant applications.

Content of Affidavits

In 1997-98, the Federal Court requested that certain sources of information provided in support of warrant applications be specifically identified in the affidavits. We were informed that this practice was adopted by the Service for all subsequent affidavits.

Findings of the Committee

Warrant Preparation

From a comprehensive listing of all warrants executed in the region for the period under review, the Committee chose three applications relating to two target groups in the

The Warrant Process

In order to obtain warrant powers under Section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court with a sworn affidavit justifying the reasons why such powers are required to investigate a particular threat to the security of Canada. The preparation of the affidavit is a rigorous process involving 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 the submission to the Federal Court. This process has evolved over the past several years with a view to ensuring that the facts, and statements of belief based on those facts, are accurate.

counter terrorism area.[14] Among these, we identified a number of statements made by the Service which accurately reflected neither the operational nor the open source information available to the Service.

In the first application we reviewed, our initial findings were that there were a large number of inaccuracies and unsubstantiated statements in the affidavit. The Service subsequently provided the Committee with additional material to substantiate the problematic allegations. We reviewed the additional material and found that most of the allegations were, in fact, substantiated by the documents provided by CSIS.

However, certain allegations remained of concern and, in our view, were not an accurate reflection of the operational and open source information available to the Service: the affidavit presented a confused picture regarding the source of certain information, and some information lacked corroboration.

The other two applications also contained several allegations that were not, in our view, sufficiently supported: the known facts did not lead to the Service's conclusions, support for certain facts was insufficient or the allegations were based on outdated information. With respect to the two latter problems, the Service reached a similar view. We were informed that in the last case, the statement we questioned was not included in the subsequent warrant application against the target group.

With respect to the warrant preparation process in general, the Committee remains seized with the issue. In two previous reports we have noted deficiencies in some past CSIS applications for warrant powers. Since proper affidavit preparation is key to the integrity of the targeting and investigatory process, it is a matter the Committee regards with utmost seriousness.

We noted that among the warrant applications reviewed for this and previous audits, the recent affidavits were much improved in all respects. The Committee is hopeful that these improvements reflect the refinements made of late to the Service's warrant preparation process.

Since proper affidavit preparation is key to the integrity of the targeting and investigatory process, it is a matter the Committee regards with utmost seriousness.

Warrant Implementation

The Committee reviewed the Service's use of warrant powers in the region and found that their implementation complied with all of the terms and conditions contained in the warrants.

Warrant Tracking

The process by which CSIS tracks warrant applications is also of interest to the Committee. Kept in diary form, the records of the warrant process provide additional assurance that all mandated procedures have been correctly followed. For the period under review, the Committee identified no anomalies in the warrant tracking records.

Quality Control in Reporting

Because intercept reports can provide the basis for requests to continue warrant operations and for targeting authorities, the accurate reporting and transcription of material generated by warrant intercepts is vital.

In this year's regional audit we found that the region in question was conducting quality control audits in accordance with the 1997 national draft policy.

We learned that the region had taken steps to ensure the quality of the reporting done by its analysts. For example, the quality control program in the region not only offered training to new analysts on quality reporting, but conducted regular performance evaluations and formalized assessments through audits.

We reviewed all requests from the Service for Ministerial approvals involving operations in the Region, and all requests to senior managers involving "sensitive institutions".

Audit of Sensitive Operations

The very nature of sensitive operations dictates that they are subject to relatively frequent Ministerial Direction. In addition, policy for implementing sensitive operations is set out in some detail in the CSIS *Operational Policy Manual* and all requests for sensitive operations, depending on the level of sensitivity, require the approval at the very least of Service senior management.

In the course of the Committee's regional audit, we examined a set of randomly selected human source operations. In addition, we reviewed all requests from the Service for Ministerial approvals involving operations in the Region, and all requests to senior managers involving "sensitive institutions"—that is, operations touching on legitimate dissent, illegal activities, and certain other matters.

Findings of the Committee

Although the policy implications of one case initially concerned us, we ultimately concluded that all source operations we intensively examined complied with legislation and Ministerial Direction. We will, however, pursue further inquiries about another investigation that had come to our attention during this review.

Internal Security

Breaches of internal security can have a catastrophic impact on an intelligence service and upon the security interests the agency is meant to guard. In CSIS, internal security is the responsibility of the Director General of Internal Security, who directs internal security officers at Headquarters and in each regional office. When it is determined that a security breach has taken place, the Director General or her representatives, investigate and recommend remedial measures.

For the fiscal period 1997-98, the Committee examined cases of suspected and actual security breaches in one region, and reviewed the security measures in place in the same regional office.

Breaches of Internal Security

We found several security issues that concerned us. In the first instance, a Service employee had inappropriately disclosed operational information. We had qualms about how CSIS had conducted its investigation. In pursuing our review, we received an

extensive explanation by CSIS about its actions, and we asked the Director to personally respond to questions about the management of the case. We learned that the matter had been considered at the highest levels of the Service.

After duly considering all of the information, we concluded that CSIS had taken appropriate action and had handled the case in a fair manner.

The second case involved the temporary loss of classified information. The incident arose from the mistaken belief among employees that they needed to follow certain procedures when transferring information. Following the incident, CSIS changed its procedures for handling data, and provided corrected instructions to its employees.

We also examined other less serious cases. Among them were allegations of unauthorized browsing in the CSIS computer data base. In one case, the internal investigation determined that the employee had a legitimate need for most of the access requests, although some minor security violations were identified. The other allegations of security violations proved to be unfounded.

Table 1
New and Renewed Warrants

	1996-97	1997-98	1998-99
New Warrants Granted	125	72	84
Warrants Renewed/Replaced[15]	163	153	163
Total	288	225	247