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

Report #123

Every year the Committee audits the entire range of the 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 main questions:

- 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 information that was strictly necessary to report or to advise the government on a threat?

METHODOLOGY OF THE AUDIT

In the region at issue, the Committee selected nine investigations at random—five counter terrorism cases and four counter intelligence cases. We reviewed all files and operational messages in the Service's electronic database and interviewed the regional managers who oversaw the investigations.

FINDINGS OF THE COMMITTEE

In all nine cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The levels of investigations were proportionate to the threat-related activities of the targets and the Service collected only the information that was strictly necessary to advise the government. During the course of the audit, two counter intelligence investigations, one of quite long-standing, were terminated. Based on our review of the intelligence collected during the period under review, the Committee concurred with the Service's decisions in both cases.

Two of nine investigations we examined did raise matters of concern:

- An instance where the request for targeting approval presented a fact inconsistent with the

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 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 their 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.

information the Service had collected. Although the Committee determined that the discrepancy did not undermine the legitimacy of the targeting authorization, we again emphasized to the Service its ongoing responsibility to ensure that facts presented in requests for targeting accurately reflect the information it holds.

- Contrary to the Service's operational policy, the regional office failed to submit an assessment report following the termination of a counter terrorism investigation. The Service attributed the lapse to an administrative oversight and has taken measures to prevent a reoccurrence.

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 that require their use. As part of its regional audit, the Committee reviewed how the Service implemented the warrants obtained in that region. Our goal was to ensure the Service's compliance with all warrant clauses and conditions.

FINDINGS OF THE COMMITTEE

Warrant Implementation

The Committee reviewed all active warrants in the Region during the period under review. In one of the warrants reviewed, the Service's implementation of warrant powers was limited to intercepting a target's telecommunications. In another, CSIS elected not to make use of any of the powers granted to it. The Service decided not to seek a renewal of either warrant and ultimately terminated the investigations.

The files we examined disclosed a number of minor procedural discrepancies: an unusual delay in submitting certain reports required upon termination of an investigation, the inappropriate use of tracking and date codes on intercept reports and the failure to convene a formal "tasking meeting" as required by Service policy.

Although these issues may appear to be of little consequence, the Committee believes that disciplined logging, reporting and tracking procedures are essential if intelligence gathering is to be effective and at the same time accountable.

Quality Control in Reporting

Because intercept reports can provide the basis for requests to continue warrant operations and for the granting of new targeting authorities, accuracy in transcribing such material is vital. This year's regional audit showed that in accordance with 1997 draft policy, the region in question was conducting the appropriate quality control checks.

Audit of Sensitive Operations

The very nature of sensitive operations dictates that they are subject to 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 require the approval of Service senior management.

METHODOLOGY

For the purpose of this regional audit, the Committee examined a set of randomly selected human source operations. In addition, we reviewed all requests to senior managers involving "sensitive institutions."[11]

FINDINGS OF THE COMMITTEE

In general, the Committee concluded that the region's development and direction of sources were appropriate. However, we identified a number of shortcomings in

the Region's compliance with policy and established administrative procedures.

- A situation with the potential to bring discredit to the Government of Canada was not reported to the Deputy Director of Operations in accordance with operational policy.

- The regional office under review failed to obtain formal prior approval from Human Sources Branch before directing a source to travel to another region for the purpose of providing operational assistance to that regional office.

- For what the Committee regards as an unnecessarily extended period, a Regional Office failed to complete an important form required by policy. While satisfied with the measures taken by the Region to rectify the problem, we believe that the Service should have taken measures earlier to ensure compliance.

- The Region was consistently late in providing certain reports, reviews and forms to CSIS Headquarters. The Service stated that its recent implementation of a new tracking system had eliminated the gaps in filing.

Internal Security

The Committee's audit of security procedures in the office under review identified two potentially serious matters. Timely intervention by management in the Region ensured that the incidents did not escalate and that more serious violations were averted. We determined that the office's internal security practices and procedures were generally sound and noted that in response to incidents elsewhere in recent years, the Region had implemented CSIS Headquarter's new procedures in relation to managing classified documents and electronic storage media.

The Committee did note, however, that the Region had conducted significantly fewer (in proportion to the staff complement) random searches of employees entering or leaving Service premises than CSIS offices in other regions. Given the security breaches of recent years, and the Service's acknowledgment of the role of random searches in increasing "security awareness" among its employees, the Committee believes the Region should bring its security practices into line with other of the Service's regional operations.

> **The Committee recommends that the Region increase the number of random searches to reflect the current practices in other CSIS regional offices.**

C. Inside CSIS

Warrants and Warrant Statistics

Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone their use bears continued scrutiny, a task the Committee takes very seriously. In addition, the review process provides insight into the entire breadth of CSIS investigative activities and is an important indicator of the Service's view of its priorities.

The Committee compiles statistics based on a quarterly review of all warrant affidavits and warrants granted by the Federal Court. Several kinds of information are tracked annually, such as the number of persons and number of locations subject to warrant powers. Table 1 compares the number of warrants over three fiscal years.

The Service did not seek renewal of any of its warrants during 1999–2000. The Federal Court issued 29 urgent warrants; however, none were renewed or replaced