B. Annual Audit of CSIS Activities in a Region

Every year the Committee audits the entire range of CSIS's investigative activities—targeting, special operations, warrants, community interviews and sensitive operations—in a particular region of Canada. Such a comprehensive examination provides insight into how the Service employs the various investigative tools at its disposal and allows the Committee to assess the ways in which Ministerial Direction and CSIS policies are implemented by the operational sections of the Service.

Targeting of Investigations

The targeting portion of the regional audit reviews how the Service applies its duties and functions as set out in sections 2 and 12 of the *CSIS Act*. The day-to-day management of investigations is governed by both Ministerial Direction and CSIS operational policies.

In reviewing the appropriateness of any Service investigation, the Committee uses three main criteria:

1) Did the Service have reasonable grounds to suspect a threat to the security of Canada?

2) Was the level and intrusiveness of the investigation proportionate to the seriousness of the target's threat-related activity?

3) Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?

METHODOLOGY OF THE AUDIT

Seven investigations were selected for this year's audit—five counter terrorism and two counter intelligence. The Committee examined all files and electronic documents associated with each of the seven cases. We interviewed both the regional managers directly responsible for the investigations and supervisory headquarters staff.

FINDINGS OF THE COMMITTEE

Based on the information reviewed, the Committee was satisfied that in all seven cases the Service had reasonable grounds to suspect a threat to the security of Canada. Neither the files and operational messages we examined nor the interviews we conducted gave any indication that the levels of investigation were out of proportion to the perceived threats.

We also reviewed the information collected in all seven cases. In one instance, certain data collected raised concerns as to whether they met the "strictly necessary" test. Although the Service provided an explanation, the Committee was not

Management of Targeting

Target Approval and Review Committee

The Service's 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 that are related to, or emanate from, that specific issue.

entirely satisfied with that response. We believe that the information collected did not meet the strictly necessary test, and we were not satisfied that, in this instance, the Service had adhered fully to the existing operational policies and guidelines governing collection.

Warrant Implementation

Under section 21 of the *CSIS Act,* only the Federal Court can grant CSIS the warrant powers required to use the most intrusive investigative procedures available to it, such as telephone or mail intercepts. Every year the Committee reviews how warrants are implemented in a number of cases selected from the files of a particular region.

The Committee's review involves assessing:

- how the Region used the warrant powers granted by the Federal Court;
- whether the Region complied with all clauses and conditions contained in the warrants;
- whether the Region's implementation of the warrants was carried out in accordance with the Act, CSIS policy and Ministerial Direction.

FINDINGS OF THE COMMITTEE

Warrant Implementation

The Committee's review of the selected warrants and the associated investigation files revealed no instances of unnecessary use of warrant powers. All collection activities were carried out in accordance with the clauses and conditions contained in the warrants. However, with respect to the Service's collection and retention of product from certain warrants, the Committee identified possible anomalies in two of the cases reviewed.

All collection activities were carried out in accordance with the clauses and conditions contained in the warrants

In the first, the Committee questioned why the Service retained a particular kind of data beyond the standard period established in CSIS operational policies. In response, the Service advised the Committee that the special retention was authorized so that assistance could be rendered to an allied agency's investigation of a terrorist network.

The second case concerned the intercepting and reporting on the communications of persons not named in the warrant. In both instances where this appeared to have taken place, the Committee subsequently was satisfied with the Service's explanation that both interceptions were appropriate and within the law (one under the provisions of the "basket clause" and the other because the intercepted person qualified as a "Vanweenan"[1]).

Shortage of Special Resources

The Committee's examination of the Region's investigation files showed that the Region suffered from the shortage of a particular expert resource. Although the resulting delays had no adverse effects in the cases we examined, the Committee would not wish to see a delay in processing unduly hinder the timely distribution of important information to appropriate officials. The Committee has expressed similar concerns in the past, and we are encouraged by the Service's initiatives to remedy the situation in this Region.

Audit of Sensitive Operations

Using human sources in collecting information is essential to effectively investigating threats to public safety and national security. However, the sensitivity of such operations is such that they are the subject of special Ministerial Direction. In addition, the procedures for implementing sensitive operations are set out in some detail in the CSIS *Operational Policy Manual*. All requests for sensitive operations, or for investigations involving "sensitive institutions" require the approval of Service senior management.[2]

---

1. The basket clause permits intercepting communications of persons who, while not named in a warrant, may be present at a location named in the warrant. The legality of the clause was upheld by the Supreme Court of Canada in *R v. Chesson*, [1988] 2 S.C.R. 148. Affirmed in the same judgement was the legality of intercepting a person named or described ("spouse" or "colleague", for example) in the warrant but not specifically targeted, likely to have regular contact with the target, and whose communications the investigating agency has reasonable grounds to believe may assist the investigation. The name of one of the parties to the "Chesson" case—Vanweenan—has since come to denote this category of persons.

2. Sensitive institutions are defined as trade unions, the media, religious institutions and university and college campuses.

METHODOLOGY OF THE AUDIT

The Committee reviewed a set of randomly selected human source operations as well as all requests to senior managers involving sensitive institutions. In each instance, we examined all files related to recruiting, developing and directing the human source in question. The purpose of the review was to assure ourselves that in handling human sources and conducting investigations involving sensitive institutions, the Service had complied with the Act, Ministerial Direction and its own operational policies.

FINDINGS OF THE COMMITTEE

With respect to both the Region's development and direction of human sources and its investigations involving sensitive institutions, the Committee concluded that the Service's actions were reasonable, appropriate and necessary for properly fulfilling its mandate.

We did identify, however, an area where the Regional office had not fully complied with Service policies governing certain administrative procedures. The Committee believes that periodic verification by Regional office management could have avoided this administrative shortcoming.

Internal Security

OVERVIEW

The Committee's inquiries showed that, within the Regional office, the level of awareness about security was generally high, and that management had undertaken appropriate measures to ensure vigilance among Service employees. We did observe, however, that the Region had conducted significantly fewer random luggage searches of its employees than CSIS offices in other regions. The Service informed us that for fiscal year 2001–2002, the Region's objective is to conduct luggage searches monthly.

> The breach occurred because the two Service employees involved left their vehicle out of sight and unattended

A BREACH OF SECURITY

The Committee examined the files regarding a security breach case that occurred during the period under review. The breach involved the theft of classified assets and material from an operational vehicle. Our review showed that the Region and

CSIS Headquarters internal security representatives had effectively investigated the incident, and that appropriate remedial measures had been taken to reduce the potential for similar security breaches in the future.

Two matters concerning the case drew the Committee's attention. First, the breach occurred because the two Service employees involved left their vehicle out of sight and unattended, which was, in the Committee's view, a lapse in judgement. Second, although in the wake of the incident the Service subsequently made constructive changes to security policies and procedures, the Committee believes that some unnecessary ambiguities remained that had the potential to weaken the policy overall.

Responding to the Committee's observations, the Service asserted that the breach did not stem from a lapse in judgement, that its employees had taken all necessary precautions and followed all established procedures and, moreover, that no disciplinary actions were contemplated. The Service agreed to adjust its policy manual to reduce the possibility of misinterpretation.