The Committee did take issue with the fact that the investigation was set in motion in the first instance.

Committee saw no evidence in the documents to sustain that premise.

The Service has acknowledged that while it was unaware of any extremists or their supporters in Canada at the time, threats of violence from extremists overseas remained a concern, as did a potential indirect threat to Canadians living overseas. The Committee noted, however, that the content of interviews focused on what was happening in Canada, not on the events taking place abroad.

In any event, the investigation failed to corroborate the original information or to identify possible affiliates of extremist organizations in Canada. The Service subsequently elected to allow the investigation to conclude upon the expiry of the targeting authority and stated that it would monitor any future developments related to the threat via its other investigations.

Development of written policies for community interviews

The Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program

The Committee is pleased to note that the Service acted on a previous SIRC recommendation and elaborated a policy which would compel investigators to inform interviewees that their cooperation is voluntary.

As in previous years, the Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program. The correspondence that CSIS sent us to explain the issue was helpful, and we believe the Service should consider adding the information to its policy.

> The Committee recommends that the definition of community interview programs be clearly set out in CSIS policy.

In a related policy matter which remains unresolved, the Committee recommended in its last audit that the Service update its *Operational Policy Manual* to include an existing memorandum on procedures for community interviews. We have seen no corporate policy revisions in this area to date.

C. Inside CSIS

The third part of this section dealing directly with what CSIS does and how it does it, consists of the Committee's comments and findings on how the Service manages its own affairs and its relations with other agencies of Government and other national governments.

Statistics on Operational Activities

By law, the Committee is obliged to compile and analyse statistics on the operational activities of the Service.

Annually, the Service provides the Committee with statistics in a number of areas: warrants, sensitive operations, finances, person-year usage and the like. We compare them against the data from previous years and question CSIS about any anomalies or new trends that we identify.

New classification system undermines Committee analysis

In 1996-97 we learned that the Service modified its statistical collection categories in the counter intelligence area. Under the old system, the categories were mainly geographically based, and as such were readily linked to identifiable targets. Under the new system, the statistics are subsumed under "themes" — economic espionage, political espionage, military espionage, foreign intelligence, proliferation, and foreign interference.

CSIS stated that the modifications were due, in part, to efforts to respond better to Cabinet Direction. However, the Committee found that many of the new definitions were unhelpfully vague and effectively undermined our ability to compile and analyse the necessary statistics.

For example, under the new system, a foreign intelligence service that uses a source to obtain information from an elected official might fall under "political espionage."

In addition, the new categories sever the statistical measures of investigations from readily identifiable targets, and because the titles are no longer standard, they make multi-year comparisons impossible.

The Committee, therefore, has asked CSIS to provide us with all of the statistical data by standard geographic, in addition to the new thematic, classifications.

. . . many of the new definitions were unhelpfully vague and effectively undermined our ability to compile and analyse

Warrants and warrant statistics

Collecting and evaluating information on warrants is viewed by the Committee as an important task. Warrants are one of the most powerful and intrusive tools in the hands of any branch of the Government of Canada; for this reason alone their use bears continued scrutiny. In addition, the kinds of warrants granted and the nature of the targets listed provide insight into the entire breadth of CSIS investigative activities and are an important indicator of the Service's view of its priorities.

Table 1 compares the number of warrants over three fiscal years.

Table 1
New and Renewed Warrants

	1994-95	1995-96	1996-97
New Warrants Granted	85	32	125
Warrants Renewed/Replaced	130	180	163
Total	215	212	288

In 1996-97, the number of new warrants rose dramatically to 125, a substantial increase attributable to the restructuring of the warrants.[22] The Service drew up affidavits requesting warrant powers in additional areas of investigation, resulting in the Federal Court granting a number of new warrants. In addition, Federal Court warrants are now required for new types of inquiry.

The number of persons affected by CSIS warrant powers has increased slightly because of the addition of the new areas of investigation. Foreign nationals continue to constitute the majority of persons subject to warrant powers.

Foreign nationals continue to constitute the majority of persons subject to warrant powers

Regulations

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations concerning how the Service may apply for warrants. In fiscal year 1996-97, no new regulations were issued.

Federal court warrant conditions

All warrants granted by the Federal Court contain conditions which the Service must follow in their execution. In 1995-96, there were a number of revisions and additions to the conditions attached to CSIS warrants. The Federal Court made one amendment and added two restrictions on how the Service can execute warrants in one type of warrant, and narrowed the manner in which the Service is able to execute warrant powers in another. Finally, three new conditions were laid down by the Federal Court which served to restrict certain types of warrants.

As we noted in the section on warrant implementation, the Committee continues to monitor changes in warrants and the powers associated with them.

CSIS Finances

On an annual basis, the Service provides the Committee with basic information on CSIS funding, and over the course of the year, we also examine any funding problems that come to our attention.

Table 2 shows spending by CSIS over the last six years:

Table 2
Actual Expenditures ($000)

	Personnel	Other Expenditures	Capital	Total
1992-93	124,926	72,591	27,833	225,350
1993-94	118,819	77,282	48,190	224,291
1994-95	115,579	71,715	18,381	205,675
1995-96	110,723	69,048	4,383	184,154
1996-97	100,153	65,287	0	165,440
1997-98[23]	99,751	65,243	0	164,994

22. In our 1995-96 *Annual Report*, we pointed out that warrant statistics do not reflect how many persons are affected by warrant powers. One warrant can involve many people, while several warrants may not mean an increase in the number of people affected.

23. *Main Estimates, 1997-98*

"Other Expenditures" includes expenses under "Construction and Acquisition of Land, Buildings and Works", and "Machinery and Equipment." Significant amounts were expended to upgrade CSIS computers. In 1997-98, for the first time, CSIS will pay $2.4 million to Public Works and Government Services Canada for grants to municipalities in lieu of the payment of property taxes. The amount was formerly paid out of the Department of Public Works budget.

CSIS has been subject to significant budgetary cutbacks. In the course of the year, the Committee asked for and received a special briefing on the effect of cutbacks on the ability of the Service to cope with rapid change.

CSIS Operational Branches

Counter Terrorism (CT) Branch

The Counter Terrorism Branch is one of the Service's two main investigatory sections (the other being Counter Intelligence) and its role is to provide the Government of Canada with advice about emerging threats of serious violence that could affect the national security of Canada. The threat from international terrorism continues to be associated with what are termed "homeland" conflicts. As CSIS has pointed out, many of the world's terrorist groups have a presence in Canada, where they engage in a variety of activities in support of terrorist movements.[24]

Since our last annual report, there have been no significant changes to the Counter Terrorism program.

Although public security remains the Service's main focus, the Branch has had to respond to government-wide fiscal restraint and budget reductions.

According to CSIS, proposals for restructuring the Branch were approved by the Service's Executive in November 1996. The proposals were consistent with the ongoing effort to make the structure of the Branch more efficient and to ensure that the maximum number of resources are directly employed in addressing the terrorist threat to the security of Canada.

The modifications in structure and operations were implemented in May 1997; their impact on the Service will be examined by the Committee in future audits.

Threat assessments

Originating primarily within the CT branch, CSIS provides other departments and agencies in the Federal Government with information about potential threats to national security by issuing threat assessments. In 1996-97, the Service brought forth 540 threat assessments, down from 602 produced the previous year.

CSIS stated that it could not attribute the decline to any specific cause. The volume of threat assessments is contingent on a number of factors beyond the Service's control: the number of foreign visitors whose presence in Canada is cause for warning; the volume of requests received from other government departments and agencies; and the number of threats identified during the year.

Many of the world's terrorist groups have a presence in Canada, where they engage in a variety of activities in support of terrorist movements

24. CSIS *1996 Public Report.*

CSIS provides other departments and agencies in the Federal Government with information about potential threats to national security by issuing threat assessments

Counter Intelligence (CI) Branch

Counter Intelligence Branch monitors threats to national security stemming from the espionage activities of other national governments' intelligence operations. By fiscal year 1996-97, the CI Branch was no longer investigating many former adversaries and intelligence services in what, since the end of the Cold War, have become emerging democratic states.

Instead, the Branch was pursuing a strategy of encouraging such agencies to act with more "transparency." That is, in its pursuit of liaison relationships with former and even current adversaries, the Branch has sought to find common ground for cooperation and information sharing.[25]

In May 1996, Canadians learned about a Counter Intelligence Branch success: the arrest of the Lambert couple (Dmitry Olshevsky and Elena Olshevskaya). The Lamberts were trained "illegals" — spies who entered Canada illegally and assumed false Canadian identities.

During 1996-97, the number of intelligence officers in the Counter Intelligence Branch rose slightly. The Service states that the Branch is focusing its resources on the areas of transnational crime, economic security, and issues surrounding the proliferation of weapons.[26] Where formal agreements are in place, the Service has strengthened its liaison relationships with foreign agencies to share information in these areas.

Analysis and Production (RAP) Branch

The Service's research arm, the Analysis and Production Branch, underwent a major reorganization in 1996-97. The goals of the reorganization were two: to improve the coordination of intelligence production with the Privy Council Office's Intelligence Assessment Secretariat,[27] and enhance the intelligence support to the main consumers of its product inside the Service — the operational desks, the Executive, Security Liaison Officers, and the like.

The Analysis and Production Branch adopted a new structure with three divisions: one responsible for counter intelligence and foreign intelligence matters, a division that deals with counter terrorism matters, and a division to prepare documents such as the public annual report and the classified annual report to the Solicitor General.

The Branch received no additional resources with which to operate. The Strategic Analysis Unit was disbanded and its analysts integrated within the other units as "experts in residence." A new unit was established to deal with foreign intelligence.

The Branch states that it is seeking to play a more proactive role by improving its dialogue with consumers of foreign intelligence products and those who set the Government of Canada's foreign intelligence requirements. The Branch now employs a standardized format for its reports, with a shorter turnaround time for production.

25. The Service's Foreign Liaison program is the subject of a special report beginning on page 3.

26. The Service's efforts in regard to threats to Canada's economic security are subject of a special report at page 11.

27. The Intelligence Assessment Secretariat of the Privy Council Office (PCO) produces foreign intelligence assessments. It coordinates the interdepartmental activities and assessments of the Intelligence Assessment Committee, chaired by the Executive Director, whose membership is composed of senior officials from the departments and agencies most concerned with intelligence matters.

The Analysis and Production Branch has become more involved in "environmental scanning" activities. Using publicly available information, the Branch analyses foreign disputes to assess the potential of these conflicts to impact on Canadian interests.

Arrangements with Other Departments and Governments

Domestic arrangements

In carrying out its mandate, CSIS cooperates with police forces, and federal and provincial departments and agencies across Canada. As outlined earlier in this year's audit report,[28] the Service may conclude cooperation agreements with domestic agencies after having received the approval of the Minister. Usually, the agreements pertain to exchanges of information, and less frequently, to collaboration in the conduct of operations or investigations.

Currently, CSIS has twenty-four arrangements with Federal Government departments and agencies, and eight agreements with the provinces. CSIS also has a separate arrangement with several police forces in one province. The Service is not required to enter into a formal arrangement in order to pass information or cooperate on an operational level with domestic agencies, though Ministerial approval for such contacts is required. It is the usual practice for the Service to enter into a formal arrangement when the other party requires terms of reference or the setting out of agreed undertakings.

Arrangements for 1996-97

The Service signed no new agreements with domestic agencies in fiscal year 1996-97 and stated that all of its current agreements were working well. In the course of our review of CSIS operations the Committee identified no significant concerns with regard to domestic agreements.

An agreement which expired in 1994 has not yet been renewed and no consultations to accomplish its renewal were held during the audit period. However, cooperation between the Service and the agencies covered by the previous agreement has continued without difficulty, with the approval of the Minister.

Information exchanged with other domestic agencies

Annually, the Committee reviews the information CSIS exchanges with other bodies in Canada in order to ensure that the Service is collecting and disclosing information in conformity with the *CSIS Act*, Ministerial Direction and Service policy.[29] In particular, we review whether,

- the threat is balanced against the infringement on personal privacy resulting from the passage of information;
- the exchange of information is strictly necessary to meet the Service's operational requirements pursuant to section 12 of the *CSIS Act;*

The Service may conclude cooperation agreements with domestic agencies after having received the approval of the Minister

28. See Section 1, "Annual Audit of a Region" discussion of Ministerial approval for intra-government cooperation.

29. Under the *CSIS Act*, the Service is to cooperate with federal and provincial departments and agencies (section 17), and disclose information [section 19(2)] "for the purpose of the performance of its duties and functions." Operational cooperation with other government institutions includes the exchanges of information, the provision of operational assistance, and can include the execution of joint operations. Section 38(a)(iii) of the *CSIS Act* states that the Committee has a duty, "to review the arrangements entered into by the Service pursuant to subsections 13(2) and (3), and 17(1) and to monitor the provision of information and intelligence pursuant to those arrangements."

- the information exchanged consists of unnecessarily personal and sensitive information, such as medical or welfare records;
- the information exchanged is reasonable, and factually accurate;
- all CSIS disclosures of information are in accordance with the preamble to subsection 19(2) or paragraphs 19(2)(a) to (d); and
- the information that CSIS provides is within the mandate of the agency receiving it.

The Committee questioned both the relevance of the reports to threats to the security of Canada and the necessity for the Service to collect them

Methodology of the audit

For calender year 1995, the Committee examined approximately 5,000 exchanges of information with other government institutions, such as the police, federal and provincial departments and agencies. All disclosures made under section 19 of the *CSIS Act* were also reviewed. We conducted on-site reviews in two regional offices in order to assess the status of cooperation between CSIS and other agencies in those regions.

Findings of the Committee

We found that the majority of the CSIS exchanges of information in 1995 were within policy parameters and statutory requirements. Several issues, however, require comment.

Collection of information on advocacy

The nature of a set of reports a regional police force gave to CSIS, and the Service's subsequent handling of them, gave rise to Committee concerns. The reports commented on a series of events that involved public advocacy or protest. The Service had deposited all of the reports into the Service's operational (section 12) data base. However, on review of the reports' contents, the Committee questioned both the relevance of the reports to threats to the security of Canada and the necessity for the Service to collect them in order to fulfill its role in advising the government.

The Committee notified the Service of its concerns, following which, CSIS agreed to delete three of the four reports. CSIS believes that the remaining report contains section 12 information. The Committee remains of the view that the outstanding report should also be removed from the operational data base, since the activities reported upon are not related to a Service investigation.

In regard to the collection and retention of information of this type generally, the Committee believes that existing Service policy does not provide comprehensive guidance to its officers.

> We recommend, therefore, that the Service review and set out policy which addresses gaps in current policy pertaining to information exchanges with police agencies in relation to advocacy, protest, and dissent.

The Committe will continue to monitor the situation.

Clarification of separate mandates

In the course of its investigations, the Service interviewed managers in two government departments. On reviewing the files on this matter, the Committee was not able to

determine whether the interviews had an operational (section 12 of the *CSIS Act*) or security screening-related (section 15) purpose. In response, the Service stated that its policies did delineate between these types of investigations; the Committee's view differs and our concerns remain.

The *CSIS Act* clearly defines two kinds of investigatory powers for the Service, each with its own array of managerial and legal tests and controls. The Committee believes that any blurring of intent between these two quite separate functions wherein information collected with one stated purpose is used for another, raises concerns about the taking of administrative "shortcuts" and invasion of privacy.

> We recommend, therefore, that the Service take the necessary measures to ensure that section 12 and section 15 investigations are clearly distinguishable, and, where they may of necessity overlap, ensure that all the applicable tests and controls are in place.

Our recommendation is directed at CSIS practice, rather than policy. The Committee intends to pay continued special attention to this issue.

Non-compliance with an information exchange agreement

Under a written agreement with a particular Federal Government department the Service has access to certain information acquired by the department. Under the agreement, an official of the department is designated as the point of contact between the agencies.

In its review, the Committee became aware of a case where CSIS by-passed the designated person and communicated directly with another employee of the department, thus–in the view of the Committee–contravening the agreement. The Service is of another view generally about such agreements, in that it regards designated persons as facilitators who may be used in the liaison role, but who are not the only persons CSIS can approach for information.

The Committee regards its own interpretation as the correct one. Where the Service has reached a formal agreement covering section 12 investigations with a government department or agency — the main purpose of which is to set out terms and conditions governing the relationship — the Service is obliged to comply strictly with the terms of that arrangement.

Non-compliance with requirements for accessing personal information

In order for the Service to access personal information acquired by a Federal Government department or agency, the Service is required to file a request through section 8(2)(e) of the *Privacy Act*. The Committee has identified three cases where, in our opinion, CSIS did not comply with the *Act.*

In one case, the Service did not agree with the Committee's view that the information at issue was personal in nature. The Committee continues to hold to its original position.

We found that the majority of the CSIS exchanges of information in 1995 were within policy parameters and statutory requirements

In respect of the other two cases, the Service stated that while the information was personal in nature, it did not originate as a government record and thus was not subject to the requirements of the *Privacy Act*. The Committee's review of the information led us to conclude differently: the opinions collected by the Service were in our view based on information acquired in the government workplace, and the Service should have filed an information request in these cases as well.

Policy and direction

In 1995, there was no new Ministerial Direction related to domestic agreements and cooperation or exchanges of information
.
There were two changes to CSIS policy with implications for interagency cooperation. In the first, the Service issued written policy on operational cooperation with other Canadian government institutions. The policy formalizes current practice and thus does not call for comment from the Committee.

The Director of CSIS will now report all disclosures made in the national interest (special disclosures) to the Committee.

The second policy issued, responds to a recommendation in the Committee's 1992-93 report, which addressed the issue of "special disclosures" by the Service. As a general principle, the Service is restricted as to whom it may disclose information. CSIS may make special disclosures to persons outside of government, at the request of the Solicitor General.

At the time, the Committee recommended that special disclosures meet the same test as disclosures made under section 19(2)(d) of the *CSIS Act*; that is, the Committee should be notified when they are made. Under the new policy, the Director of CSIS will now report all disclosures made in the national interest (special disclosures) to the Committee.

International arrangements

Pursuant to section 17(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General — after consultation with the Minister of Foreign Affairs and International Trade — before entering into an arrangement with the government of a foreign state or an international organization. During the exploratory and negotiating phase leading to an agreement, no classified information is exchanged.

Arrangements for 1996-97[30]

As of 31 March 1997, the Service had a total of 203 arrangements with 123 countries and three international organizations. During the year, the Minister approved one new arrangement with a foreign agency in Asia and three existing arrangements were expanded. Two of the three agencies' predecessor organizations (both in countries on the same continent) had poor human rights records; the revised agreements will allow for consultation and technical assistance.

Information about transnational crime

A number of intelligence agencies abroad collect information about trans-national crime. One of the functions of CSIS Security Liaison Officers posted abroad is to develop and maintain the inter-

30. The broad scope of the Service's foreign liaison and cooperation activities are subject of a special audit report in Section 1, page 3.

agency relations required to facilitate the exchange of this information.[31] In turn, the Service passes the information on to the appropriate law enforcement authorities in Canada.

Collection of Foreign Intelligence

Foreign intelligence is information concerning the "capabilities, intentions or activities" of a foreign state. Under section 16 of the *CSIS Act*, the Service may, at the written request of the Minister of Foreign Affairs and International Trade or the Minister of National Defence, collect foreign intelligence.

Methodology of the audit

The Committee employs various methods to audit the collection of foreign intelligence:

- as required by section 16 of the *CSIS Act*, we examine Ministers' requests for assistance;
- we review all information about Canadians retained by CSIS for national security purposes;
- pursuant to the "strictly necessary" requirement of section 12 of the *CSIS Act*, we assess whether CSIS has a valid reason to retain information from section 16 operations;
- in general terms, we assess whether the Service's cooperation with the Communications Security Establishment (CSE)[32] complies with the *CSIS Act*.

Committee findings

The Committee noted several new developments regarding both policy and operational matters with respect to section 16 (foreign intelligence) operations within the Service.

At the policy level, CSIS published in 1995-96 a new chapter in the *CSIS Operational Policy Manual* formalizing existing procedures.

In an operational matter, CSIS has established a new system for handling foreign intelligence reports. This new mechanism does not materially change the Committee's ability to track the manner and extent to which CSIS retains foreign intelligence.

The Committee employs various methods to audit the collection of foreign intelligence

Inappropriate use and retention of identifying information

Two cases drew special attention from the Committee. In the first, the Service sought and obtained from the Communications Security Establishment information that identified a person or organization without sufficient explanation of why it required the information.

In the second case, we identified an instance where information about a prominent individual's involvement in a morally questionable activity had been retained — improperly, in the Committee's view. We believe that the retention of the identifying information in this case was not "strictly necessary," given the potential detriment to the person.

31. For more on CSIS Security Liaison Officers see, page 3.

32. The Communications Security Establishment is an agency of the Department of Defence. As described by the Auditor General in his 1996 report to Parliament, *The Canadian Intelligence Community*, the CSE, "analyses and reports on intercepted foreign radio, radar and other electronic emissions... and provides this foreign intelligence to Canadian government clients."

We recommend that CSIS clarify its policy in regard to the "strictly necessary" requirement when assessing whether to retain identifying information from foreign intelligence in the Service's computerized data base.

Stale-dated ministerial requests

In last year's report, the Committee noted that a number of standing requests for assistance from Ministers were three or more years old, and had not been signed by the then current Ministers. The Ministers subsequently signed the requests.

Management, Retention and Disposition of Files

The Committee constantly monitors the Service's file management policies and practices

Files are the essential currency of intelligence gathering. Every CSIS investigation and every approved target requires the creation of a file, and a system for making the information in it available to appropriate officers in the Service. Balanced against this information gathering apparatus is the clear restriction on the Service set out in the *CSIS Act*, that it shall collect information "to the extent that it is strictly necessary." The Committee constantly monitors the Service's file management policies and practices to help ensure that no unnecessary information is improperly retained or distributed.

File disposition

CSIS files are held according to predetermined schedules that define how long they must be retained after Service employees cease using them. When this period expires, the National Archives Requirements Unit (NARU) in CSIS reviews the files for disposition. The staff in NARU decide whether to keep the file, destroy it, or send it to the National Archives' holdings.

During fiscal year 1996-97, NARU reviewed 12,495 files. Of these, 8,565 were destroyed, the Service retained 3,896 files, and 34 will be sent to National Archives once the retention dates are reached. This is far lower than last year's 115,000 files processed by the Unit, a decrease owing to the final disposal in the year previous of the remainder of approximately half a million files inherited from the Royal Canadian Mounted Police in 1984.

New File Statistics

Comparing new file statistics for 1995-96 and 1996-97 highlights two interesting trends:

- major decreases in the files on foreign nationals visiting Canada, where there was a counter intelligence concern; and

- increases in the number of files on screening, particularly in the categories of citizenship, immigration and refugees.

The Committee is cautious about drawing too much from these observations. A decrease or increase in the number of files does not, of itself, presage a change in the threats to national security. It may instead represent variations in individuals' memberships or group affiliations, or alternatively reflect the Service's focus on the most dangerous elements in some groups.

CSIS retention of internal E-mail

One continuing area of concern for the Committee has been the management of the Service's E-mail system. In the past, CSIS, like most large organizations, relied almost exclusively on hard copy, paper-based files. This was helpful to the Committee's research and audit activities in that all written communications within CSIS could be found in these files, including internal memoranda and notes pertaining to operations.

Recently, however, the Service has converted its information management system to a "paperless" electronic one which automatically retains formal communications within CSIS (thus retaining it for audit) but does not do so for "informal" correspondence.

Early in the new system's implementation period, the Committee noted a relative dearth of E-mail notes (the equivalent of the old hardcopy internal memoranda) normal to most operations. We subsequently learned that for the informal E-mail notes to be retained required a decision by each CSIS officer on whether to "save" the correspondence. Indeed, CSIS staff were alerted to the fact that anything they saved would be subject to review.

CSIS has since revised its instructions to employees; the new procedures appear to facilitate saving the E-mail that should be placed in the corporate record. The Committee has since noted a gradual increase in the volume of operational E-mail that we encounter in the course of our reviews. We will continue to monitor the situation.

Internal Security

In the 1994-95 SIRC Annual Report, we reported on the case of Aldrich Ames, a Central Intelligence Agency employee arrested for spying for the Soviet Union. On 16 November 1996, a second Central Intelligence Agency employee, Harold James Nicholson, was arrested for spying on behalf of Russia. Like Ames, Nicholson's motivation was financial. It does not appear that he obtained or betrayed information that can be considered injurious to Canada's national security.

As a result of the Ames case, CSIS undertook a review of its own internal security practices. The Committee received the final report of that review, *Finding the Balance*, in October 1996.

The Service's report concluded that, "CSIS maintains sound and effective security practices," and underlined the view that security procedures must be balanced against the rights of CSIS employees. The report recommends a number of changes in the areas of security clearances for CSIS staff, as well as enhanced security awareness programs, and increased physical security. In addition, the report recommends that CSIS employees be required to disclose financial information on hiring, and be subject to polygraph testing on a periodic basis.

One continuing area of concern for the Committee has been the management of the Service's E- mail system

. . . there is little empirical evidence for concluding that there is value in the increased use of the polygraph in employment screening

The implementation of new procedures for vetting security clearances for external contractors, and random searches of staff and visitors was also recommended. The Committee understands that as of the time of release of this report, most of the recommendations have been adopted.

Committee comments on matters of internal security

It is the Committee's view that employee awareness of security issues and knowledge of proper procedures is at least as important as designing new procedures. We noted that the report deferred extensive comment on the control and handling of classified documents and instead recommended that a study be conducted. CSIS informs us that the study has since been undertaken.

We also believe there is little empirical evidence for concluding that there is value in the increased use of the polygraph in employment screening. The Committee continues to hold to the opinion expressed in previous reports that a rigorous program of security checks would probably be more effective.

The Committee believes that the employee complement of CSIS should be broadly representative of Canada's population

Personnel Recruitment and Representation Within CSIS

Recruitment of personnel

The Service held two Intelligence Officer (IO) Entry Training Courses for fiscal year 1996-97 with a total of thirty participants. All but one recruit successfully completed the course. Five of the trainees were conversions from other positions within the Service.

The female to male recruitment ratio was seventeen females to thirteen males, a change from last year's ratio of ten to twenty- two. The representation of visible minorities was one male and three females.

All students met the bilingualism criteria.

Representation of Canadian population in the Service

The Committee believes that the employee complement of CSIS should be broadly representative of Canada's population. Over the past several years, we observed some progress in the Service's recruitment of certain groups, but much remains to be done.

The Service made the most progress in meeting its objectives for the employment of visible minorities. CSIS has also made some advances in employing Aboriginal peoples and persons with disabilities, although the Service did not meet the objectives it had set for itself. CSIS states that the under-representation of Aboriginal groups is a phenomenon of the Public Service at large and results, in part, from a high resignation rate. Although CSIS achieved its objective for employing persons with disabilities in 1994, the two subsequent years have been less successful.

CSIS exceeded its objectives for placing women in the management category positions in 1995, and in

the senior intelligence officer levels in 1996. Since then, however, representation of women has declined both because of resignations, and reductions in numbers of positions in management categories where women were fairly well represented. Similarly, the Committee has noted the fact that cutbacks in CSIS staff levels have had their greatest impact on the women employees in the Administration category.