Canadian Security
Intelligence Service

Service canadien du
renseignement de sécurité

Public Report

2004-2005

Canada

Public Contact

For more information, please contact:
Canadian Security Intelligence Service
Communications Branch
P.O. Box 9732
Postal Station T
Ottawa, Ontario
K1G 4G4

(613) 231-0100 (Communications)
Internet: www.csis-scrs.gc.ca

Cat No. PS71-2004
ISBN 0-662-67907-5

Think recycling

This document is printed with environmentally friendly ink

Recycled post-consumer fibre

Acid-free paper

Table of contents

The *CSIS Public Report for 2004-2005* was delayed as the Service was shifting the period of review from the calendar to the fiscal year. This report covers the period from April 1, 2004 to March 31, 2005.

A Changed World

Canada's threat environment has changed dramatically since 1984, when the Canadian Security Intelligence Service (CSIS) was created. At that time, the main global concern was the rivalry between the United States and the Soviet Union. CSIS focused most of its efforts and resources on threats posed by espionage activities, clandestine foreign interference and subversion.

In the early 1990s, transnational terrorism began to emerge as the most serious security threat. Today, terrorism is the primary focus of the Service. However, two other serious threats continue to demand attention: (1) the worldwide proliferation of weapons of mass destruction; and (2) espionage and other foreign-influenced activities.

Priorities

Terrorism

The Service's highest priority in 2004-2005 was to safeguard against the possibility of a terrorist attack occurring in or originating from Canada. Associated with this, CSIS sought to stop terrorist fundraising and related activities from occurring in Canada.

Terrorism is not new to Canada. The 1985 bombing of Air India Flight 182 was the single most lethal terrorist act in Canadian history. However, the current terrorist threat should not be underestimated. Because Canada plays a military role in Afghanistan, it is a terrorist target and has been specifically named as such by Osama Bin Laden. And while Canada has not yet been directly attacked, terrorist acts have claimed the lives of Canadians: 24 in the 9/11 attacks and 2 as a result of the 2002 bombings in Bali. More recently, Cpl. Jamie Brendan Murphy of the Canadian Forces was killed by a suicide bomber in January 2004 while on duty in Afghanistan.

Other factors contribute to the seriousness of the threat:

- Persons trained in terrorist training camps as well as veterans of campaigns in Afghanistan, Bosnia, Chechnya and elsewhere are known to reside in Canada.
- Canadians who have travelled to Iraq to fight in the insurgency may return home with new skills and new motivations.
- A relatively large number of terrorist groups are known to be operating in Canada, engaged in fundraising, procuring materials, spreading propaganda, recruiting followers and conducting other activities.
- Terrorist groups continue to intimidate and exploit Canada's immigrant and expatriate communities, sometimes through front organizations.
- Canadian residents and citizens are known to have planned operations against foreign targets, and to have personally participated in them.
- Terrorists in Canada have conducted preliminary reconnaissance against potential Canadian targets.

Canadian Terrorists Active Overseas

Abdel Rahman Jabarah was sought for his involvement in the bombing of residential compounds in Riyadh, Saudi Arabia, in May 2003. In July 2003, he died in a gun battle with Saudi security forces.

His brother, Mohammed Jabarah, was involved in a foiled plot to attack foreign embassies in Singapore. He is currently detained in the United States.

Kassem Daher was imprisoned in Lebanon for his involvement in an armed clash between a radical Islamic group and Lebanese forces in early 2000.

Abderraouf Jdey and Faker Boussora both attended Al Qaeda training camps. Jdey made a "suicide video" for Al Qaeda in which he pledged his life for the movement. Both are still at large and believed to be operationally active abroad.

Extremists and Terrorists in Canada

In 2004-2005, several citizens of other countries were held or continued to be constrained under security certificates. These included: Ernst Zundel, a leader within the Canadian and international White Supremacist movement; Mohamed Mahjoub, a member of Vanguards of Conquest, a radical wing of the Egyptian Islamic Jihad; Mahmoud Jaballah, senior operative of the Egyptian Islamic terrorist organization Al Jihad; and Hassan Almrei, Mohamed Harkat, and Adil Charkaoui, suspected of association with Al Qaeda.

The security certificate process prevents Canada's immigration laws from being misused by the few who would seek to undermine the security of Canadians and the multicultural society in which we live. It enables the government to seek removal of a permanent resident or a foreign national based on information that, if disclosed, would be injurious to national security or the safety of any person.

Certificates are used only to remove non-citizens who pose the greatest threat to Canada and Canadians. A security certificate is issued in exceptional circumstances and the measure is employed judiciously. Since 1991, only 27 certificates pertaining to 26 individuals have been issued.

Massacre in Spain

On March 11, 2004, in Madrid, 10 explosive devices were detonated on four commuter trains during the morning rush hour, killing 200 people and injuring more than 1,400.

Investigations pointed toward a cell of Moroccan nationals in Spain. Within a month, police had arrested or detained more than 20 people. Apparently, none had previously attended terrorist training camps or participated in terrorist attacks outside Spain.

On April 2, Spanish authorities thwarted an attempted bombing of the track of a high-speed train. Shortly afterward, police identified an apartment south of Madrid as the base of operations for individuals suspected in both cases. They raided the apartment on April 3; trapped inside, the suspected terrorists set off explosives, killing themselves and one of the policemen in the blast.

• • •

The explosives were found to be of the same type used in the March 11 attacks and the attempted railway bombing. It is generally assumed that the terrorists who died in the apartment were responsible for both attacks.

By the end of the year, further arrests had been made and the pursuit of other suspects continued.

Al Qaeda and Like-Minded Groups

The stated goals of Al Qaeda and similar groups are to eliminate Western influence and secular forms of government in Muslim countries, and to establish theocratic states adhering to what most commentators see as a radical and distorted interpretation of Islamic law and history.

Headed by Osama Bin Laden, Al Qaeda is an umbrella organization for a wide array of terrorist groups. It is really a network of individuals and organizations acting both independently and in cooperation with each other. The network is ever-changing, making it an elusive target for intelligence agencies.

During the reporting period, terrorists struck in many countries. Outside of Israel, Iraq and Afghanistan, the highest death tolls were in Southeast Asia (Indonesia, Thailand and the Philippines), Spain, Uzbekistan and Bangladesh. Other attacks were thwarted by authorities in several countries, including the United Kingdom, France and Italy.

A growing number of countries are experiencing attacks by terrorist groups affiliated with Al Qaeda. Because this form of terrorism ignores borders, it is characterized as transnational terrorism.

Secessionist Violence

Secessionist violence in different regions of the world can affect Canada's ethno-cultural communities. For example, the long-standing conflict in Sri Lanka has had an impact on Sri Lankan immigrants in Canada: the Liberation Tigers of Tamil Eelam (LTTE), a sophisticated organization that pioneered the use of human suicide bombers, have actively recruited and raised funds among Canada's Tamil immigrant community.

Another group with secessionist goals and links to Canada is the Kongra-Gel, a Kurdish group formerly known as the PKK. [1] In June 2004, the group renewed its campaign of terrorism against the Turkish government.

Domestic Extremism

Terrorist violence in Canada is not always related to conflicts beyond our borders. In fact, several violent campaigns have been conducted by homegrown terrorists, including the Front de libération du Québec in the 1960s and 1970s, and Direct Action, responsible for the 1982 BC Hydro and Litton Industry bombings.

Even today, a number of people are prepared to resort to violence to achieve their goals. Among these are neo-Nazis and violent fringe elements of single-issue groups from the ecological, animal-rights and anti-globalization movements. CSIS respects the rights of all to political dissent and freedom of speech. At the same time, the Service continuously assesses the potential for violence resulting from the activities of members of such groups.

The Beslan School Siege

On September 1, 2004, 33 armed terrorists took approximately 1,300 schoolchildren and adults hostage at School Number One in the town of Beslan in the Russian republic of North Ossetia.

Shortly afterward, the terrorists executed 20 adult male hostages, wired the school with explosives, and threatened to execute or blow up more hostages. They also refused to allow food, water or medicine to be delivered to the hostages. Among their demands was the withdrawal of all Russian troops from Chechnya. Attempts to negotiate an end to the standoff failed.

On the third day, amid much confusion, a massive battle took place between the hostage-takers and Russian security forces, during which the terrorists detonated their explosives. As a result, approximately 339 people were killed. At least 171 of them were children; only 11 were soldiers. Approximately 445 people were wounded. All but one of the hostage-takers died in the battle.

[1] The PKK is listed as a terrorist entity for the purposes of Part II.1 of the *Criminal Code of Canada*.

Trends and Developments

Transnational terrorist groups today are increasingly sophisticated. Many of their members are well-educated and multilingual. A growing number are skilled in modern technology and use it to communicate with each other via encrypted messages, to transfer funds electronically, and to mount cyberattacks against private-sector and government targets.

In 2004-2005, terrorists continued to:

- display a willingness to die for their cause(s);
- augment their ranks, largely as a result of the conflict in Iraq;
- launch attacks globally, including in countries not previously targeted;
- target "soft" (i.e. non-military) targets, with the aim of killing as many people as possible;
- demonstrate outstanding operational security, highly effective planning skills and the ability to run operations in several countries simultaneously;
- exploit and intimidate immigrant communities;
- attempt to acquire more lethal weapons, including chemical, biological, radiological and nuclear devices;
- further refine their use of the Internet, particularly Internet news media, as a propaganda and recruitment tool;
- equip themselves with sophisticated devices and weaponry, including rockets and missiles; and
- recruit a growing number of young, second-generation immigrants with little or no previous link to terrorism.

Organizationally, Al Qaeda and its affiliates have become increasingly dispersed and loosely linked, with far-flung elements that are more likely to act autonomously. This makes them more difficult to identify, monitor and forestall.

Despite the greater challenges, there were numerous positive developments in combatting terrorism. On the international front, these included:

- increased anti-terrorism efforts by many countries, often supported by stronger legislative/government authority and increased resources;
- increased cooperation between security and intelligence agencies, often with positive results;
- the death or capture of a significant number of terrorists;
- a diminishing number of sanctuaries for terrorists; and
- the thwarting of several potentially catastrophic attacks as a result of heightened public awareness, rapid information exchanges, and coordinated responses by security and law enforcement agencies.

On the domestic front, CSIS contributed to several successful enforcement initiatives, including information leading to arrests, removals from Canada and the tracking of terrorist financing.

Proliferation

CSIS takes very seriously the threat posed by the proliferation of weapons of mass destruction (WMDs)—nuclear, chemical, biological and radiological weapons—as well as the proliferation of systems for delivering WMDs to intended targets (e.g. missiles). Controlling their spread is a challenge requiring international commitment.

The Service works with its domestic and international partners to monitor developments around the world, and to identify countries and terrorist organizations that seek to develop, acquire or use WMDs and delivery systems. Concern has focused on several states' attempts in this direction. CSIS will continue to investigate such activities, as well as efforts by those states to procure any technology/material from within Canada that could support WMD development.

Espionage and Other Foreign-Influenced Activities

Crime Knows No Boundaries

Taking advantage of globalization and new technology, transnational criminal activity has become a growing problem throughout the world. Typical fields of transnational criminal activity include drug trafficking, migrant smuggling, corruption, arms dealing and money laundering. In some cases, the activity involves members of terrorist groups or serves terrorist interests, for example, through money laundering or weapons procurement.

During the Cold War, the Soviet bloc engaged in sophisticated political and military espionage against Western nations. Today, foreign intelligence services continue attempting to infiltrate key Canadian government departments in their quest for intelligence. At the same time, increasing global economic competition is shifting the focus to the illicit acquisition of economic and technological information. Both traditionally hostile and ostensibly friendly governments have engaged in such activity in Canada.

Today, most espionage activities directed against Canada involve economic espionage. This is illegal, clandestine or coercive activity by a foreign government to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage. Economic espionage usually targets scientific and technological developments in Canada's natural resource sector, as well as our critical economic and information infrastructures.

Because Canada is a world leader in many technology-intensive fields (including aerospace, biotechnology, chemicals, communications, information technology, mining, metallurgy, nuclear energy, oil, gas and environmental technologies), Canadian companies have been targeted by foreign governments seeking economic or commercial advantages.

Foreign countries employ various means for their economic espionage against Canada. In some cases, highly skilled professional operatives use specialized knowledge and cutting-edge technology to acquire intelligence. In other instances, countries enlist or coerce the cooperation of their citizens who are visiting Canada, such as students and scientists, exchange personnel, members of delegations, employees of state-owned corporations, and business people.

While espionage may occur within Canada, Canadian business people travelling abroad are also vulnerable. A foreign government can operate more easily within its own borders, adapting hotel rooms, restaurants, offices and telecommunications systems for espionage purposes.

Despite strong warnings from the Government of Canada, certain countries continue to use their intelligence services to manipulate and exploit expatriate communities in Canada.

Countering the activities of foreign intelligence agencies and foreign interference in Canada is a delicate and expensive task. In 2004-2005, the Service continued to dedicate substantial resources to this effort.

How We Meet Our Responsibilities

The mandate of CSIS is primarily to collect, analyze and retain information and intelligence on activities suspected of threatening the security of Canada, and to report to and advise the government.

Collecting Intelligence

CSIS collects intelligence about individuals or groups whose activities it suspects of threatening national security.

The Service draws on a broad range of sources to gather intelligence and track breaking issues that affect the security of Canadians. These include human sources, other intelligence services, law enforcement agencies in Canada and elsewhere, technical intercepts and members of the public. The Service also follows academic research closely to ensure it has the most balanced and nuanced information available about global trends. Finally, CSIS works closely with many government

departments and agencies, particularly members of the Canadian intelligence community such as the Department of National Defence, the Communications Security Establishment (CSE), Public Safety and Emergency Preparedness Canada, Transport Canada, Citizenship and Immigration Canada (CIC), the Canada Border Services Agency (CBSA), Foreign Affairs Canada, and the RCMP.

Investigative action taken by the Service is commensurate with the perceived level of the threat. Action begins with the least intrusive measures appropriate to the situation. Further steps are taken as needed, each requiring higher levels of approvals. At all times, the Service is mindful of individual rights and civil liberties, balancing them against its responsibility to protect all Canadians and Canada's national security.

Analysis and Reporting

Security intelligence is generally complex, often obscure, and normally collected in bits and pieces that separately may offer little useful information. The Service's analysts are responsible for fitting the pieces of the puzzle together. They also interpret the significance of certain information and developments, and constantly reassess the threat environment.

Analysts usually have specialized knowledge in critical fields such as terrorism, espionage, transnational criminal activity, economics, geopolitics, weapons proliferation, information technology, domestic extremism and communications.

Analysis leads to the production of two types of reports:

- **Strategic reports** are in-depth reports that give the context for specific threats and examine their wide-ranging security implications. The reports also examine emerging trends and issues that could affect the security of Canada.
- **Tactical reports** deal with specific issues or events. They address current or emerging threats to Canada or Canadian interests abroad, federal government ministers travelling abroad, internationally protected persons or other prominent visitors to Canada, foreign missions and other personnel in Canada, and special events such as G8/G7 summits. Tactical reports are often prepared in support of the Service's intelligence collection activities or at the request of a client.

The Service disseminates its intelligence products to a broad range of carefully selected Canadian government intelligence consumers and allied services.

Security Screening

Contributing to International Trade

CSIS is an active partner in Canada–U.S. border initiatives, including the Free and Secure Trade (FAST) program, initiated by the 2001 Smart Border Declaration. FAST is intended to facilitate the legitimate flow of people and goods across the border, while addressing both countries' security requirements. The program provides a pre-approved security process for importers, carriers and truck drivers to expedite their clearance through Canada–U.S. land border crossings. The Canada Border Services Agency is responsible for the FAST program; the Service undertakes security assessments of individuals (primarily truckers) seeking a FAST pass to cross the border for commercial purposes.

Over recent years, the Government of Canada has introduced policy and legislative initiatives requiring CSIS to increasingly assist government and immigration screening programs.

Immigration and Citizenship Screening

The Numbers

In 2004-2005, CSIS used its state-of-the-art automated system to process 254,364 requests under the Immigration and Citizenship Screening program. The system is regularly updated to improve its operation, meet new requirements and reflect newly available threat-related information.

As authorized by the *Canadian Security Intelligence Service Act*, the Service provides security-related services and advice to Citizenship and Immigration Canada with respect to the screening of visitors from countries of terrorist concern, as well as refugee claimants, applicants for permanent residence and applicants for Canadian citizenship. By doing so, CSIS helps prevent non-Canadians who pose risks or security concerns from entering Canada. In the case of such persons who have gained entry, the Service's contribution helps prevent them from gaining status in Canada.

CSIS fulfills these responsibilities in a number of ways:

- It vets visa applications from nationals and residents of countries that are suspected of assisting terrorists, condoning or endorsing terrorist activities, or serving as potential bases for launching terrorist operations.
- As part of the government's Front End Screening program, it checks all refugee claimants arriving in Canada against CSIS records, thereby identifying potential security cases as soon as possible in the refugee determination process.
- On request, it helps front-line port of entry CBSA officers to interview visitors and refugee claimants about whom a CBSA officer has security concerns, and offers security-related advice.

In addition, CSIS provides security screening of immigrants and refugee claimants who apply for permanent residence status from within or outside Canada. Applications originating outside Canada are handled under the Overseas Immigration Screening Program, with responsibility for security screening shared by the Service and CIC officials based abroad. Generally, CSIS becomes involved in overseas screening only if it is requested by CIC or if it receives information of concern from established sources. This approach frees the Service to concentrate on cases deemed to be higher-risk.

Last, CSIS provides CIC with security assessments on applicants for Canadian citizenship. Under this process, CIC forwards all citizenship applications to CSIS for review. The Service advises CIC if it has security concerns about a particular applicant, and provides CBSA with relevant security advice.

Government Screening

The Numbers

In 2004-2005, CSIS processed about 100,000 requests under the Government Screening Program. The average time required to process an application ranged from 30 days for Level I (Confidential) applications to 69 days for Level III (Top Secret) applications.

Under the Government Security Policy, security clearances are required for federal employees, members of the Canadian Forces or persons under contract to a government department who, in the performance of their duties, have access to classified government assets or information.

With the exception of the RCMP, which conducts its own investigations, the Service assists all government departments and agencies, including the Canadian Forces, in acquiring the necessary security clearances for their staff and contractors. In this way, it helps prevent those who pose a security concern from gaining access to classified government assets and information. The Service furnishes information and advice; under the provisions of the Government's Security Policy, individual departments have exclusive authority to grant or deny their security clearances.

The Service also undertakes security assessments for special events and some provincial security clearance programs, as well as for site access programs at airports, facilities subject to Parliament's authority and nuclear power stations.

Government screening has increased dramatically over the past two decades, in terms of the number of clearance requests and the number of clients submitting the requests. The increase is largely the result of new statutes and changed regulations, including those that have created or altered programs related to access to nuclear generation sites and restricted areas in airports, and others that involve providing security clearances for non-federal clients.

Foreign Screening

CSIS supplies security assessments of individuals to some foreign states, foreign agencies and international organizations under reciprocal screening agreements.

Requests for foreign screening typically involve:

- database checks and inquiries on Canadian residents wishing to take up residence in another country; or
- checks and inquiries on former and current Canadian residents being considered for classified access in another country.

Improving National Security Through Partnerships and Information-Sharing

The Numbers

In 2004-2005, CSIS had more than 250 relationships with foreign agencies in approximately 140 countries.

CSIS has information-sharing agreements with foreign organizations, including foreign intelligence agencies. The agreements give the Service access to intelligence that might not otherwise be available to it, and can lead to cross-training, personnel exchanges and joint operations.

Domestically as well, CSIS seeks closer ties with Canadian organizations, particularly in the intelligence community. In 2004, the biggest development in this respect was the establishment of the Integrated Threat Assessment Centre (ITAC), which is housed in CSIS facilities. CSIS supplies substantial infrastructure and administrative support, as well as emergency assistance 24 hours a day, seven days a week, through the CSIS Threat Management Centre. A functional component of CSIS, ITAC is a community resource staffed by representatives from federal and provincial organizations. It works closely with the National Security Advisor, and was created under the auspices of the National Security Policy.

ITAC serves as a single, central organization for assembling, integrating, analyzing and sharing information provided by a wide range of sources. It distributes threat assessments within the intelligence community and outside it, as required. ITAC also has liaison arrangements with its counterpart organizations in Britain, the United States, Australia and New Zealand.

Providing Client-Focused Service

CSIS representatives meet regularly with security and program officials representing departmental and agency clients. The meetings enable CSIS to provide intelligence to clients and gain a better understanding of their needs.

CSIS also has close ties with other cooperative initiatives, including the Integrated Border Enforcement Team (IBET) program. IBETs are made up of Canadian and U.S. partners, including the RCMP, the Canada Border Services Agency, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the U.S. Coast Guard.

The program began in 1996, focusing on the border between British Columbia and the state of Washington. Since then it has evolved into a cross-country enforcement initiative. Today, teams are strategically located along the length of the Canada–U.S. border. They work daily with local, state and provincial enforcement agencies to help protect Canada and the United States from potential threats of terrorism, and to combat smuggling of humans, contraband cigarettes, drugs and other illegal substances.

In addition, the Service cooperates with the RCMP's Integrated National Security Enforcement Teams (INSETs). First established in 2002 in Vancouver, Toronto, Ottawa and Montreal, INSETs serve two functions:

- They increase Canada's capacity to collect, share and analyze intelligence among partners concerning targets that threaten national security and their related criminal activities.
- They create an enhanced enforcement capacity to bring such targets to justice.

INSETs are made up of representatives seconded from the RCMP, CSIS and other partners, such as the Canada Border Services Agency, Citizenship and Immigration Canada, and provincial and municipal police services.

Earning Trust Through Accountability

Appearances by the Director of CSIS Before Parliament in 2004-2005

Date	Parliamentary body
2004	
May 6	Subcommittee on National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness (Main Estimates)
June 21	Commission of Inquiry into the Action of Canadian Officials in Relation to Maher Arar (with Assistant Director)
July 27	Interim Committee on National Security
November 24	Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness (Main Estimates)
December 14	Subcommittee on Public Safety and National Security (Bill C-36 Review)
2005	
February 22	Subcommittee on Public Safety and National Security
March 7	Senate Committee on *Anti-terrorism Act*

CSIS has an obligation to be accountable to the government and the Canadian public, and respectful of individual rights. When the Service was created in 1984, legislators sought a management style that would be responsive to political decision-makers, cooperative with review bodies and disciplined. Two thirds of the *CSIS Act* is devoted to describing how the Service's activities are to be monitored, reviewed and approved by others. In fact, the degree of accountability demanded in the *Act* sets CSIS apart from most of its counterparts around the world, making it a model for other agencies.

To ensure that CSIS activities are in compliance with the law, the Service is subject to arm's-length review by both the Inspector General of CSIS (IG) and the Security Intelligence Review Committee (SIRC). The IG and SIRC are also responsible for examining whether any CSIS operational activity involves "an unreasonable or unnecessary exercise by the Service of its powers."

SIRC performs its responsibility by identifying and reviewing a number of research projects annually in order to provide a retrospective assessment of specific CSIS activities and investigations.

"After 20 years we can say with confidence that the *Act* works well for both SIRC and CSIS. CSIS is a still-evolving—indeed, perpetually evolving—organization adapting necessarily to changes in the global environment, and SIRC must ensure that our evaluative activities evolve at the same pace."

—SIRC Report 2003–2004: An Operational Review of the Canadian Security Intelligence Service.

The IG was created by Parliament in the *CSIS Act* and reports through the Deputy Minister to the Minister. The Inspector General is responsible for monitoring the Service's compliance with its operational policies, reviewing the operational activities of CSIS and submitting a certificate setting out the degree of satisfaction with the Director's annual operational report. The certificate and the report are forwarded by the Minister to SIRC.

SIRC, which is independent of CSIS, guards against any infringement upon human rights and freedoms by CSIS. SIRC has access to any information it requires from CSIS and reports to Parliament annually. Under section 41(1) of the *CSIS Act*, anyone may make a complaint to SIRC "with respect to any act or thing done by the Service."

SIRC and the IG have sometimes taken issue with CSIS activities; in many cases, their recommendations have prompted CSIS to modify its procedures and practices.

In addition to the SIRC and IG reviews is the Service's own extensive, multi-faceted system of internal controls and accountability. This ensures that the work of CSIS is not only effective but also in conformity with the law, ministerial direction and propriety, and that it is proportionate to the nature and seriousness of security threats.

CSIS internal controls are shaped by the Service's highly centralized nature, which is reflected in operational decision-making. Two committees chaired by the Director exercise central operational control:

- The Target Approval and Review Committee decides which groups or individuals will be subject to Service investigation, and what level of intrusiveness is appropriate to each. Senior management thus is responsible for launching any investigation, and determines and controls its scope and intrusiveness.
- The Review Committee reviews and approves all warrant applications to the Federal Court under section 21 of the *CSIS Act*. Senior management thus is responsible for examining and approving any request to use the Service's most intrusive investigative powers before the request is submitted to the Federal Court. The committee includes legal representation from the Justice and Public Safety departments.

Section 20 of the *CSIS Act* requires the reporting and investigation of all cases in which CSIS employees may not have complied with legislation or policy, or may have acted unlawfully in the performance of their duties. This provision ensures that alleged unlawful activities not detected by provincial law enforcement agencies will still be reported to the Minister.

Finally, CSIS internal control mechanisms operate within a broader framework of direction and accountability.

In 2004-2005, in addition to review by external bodies and its own internal controls and accountability mechanisms, CSIS activities were reviewed by outside bodies such as the Auditor General, Parliamentary committees, the O'Connor Commission of Inquiry and Commissioners for Access to Information, Privacy and Official Languages.

"In my opinion, the Service has not acted beyond the framework of its statutory authority, has not contravened any Ministerial Directions, and has not exercised its powers unreasonably or unnecessarily."

—Extract from the Inspector General's Certificate, November 2004

Outreach to the Public

CSIS recognizes its responsibility to directly inform the public about its work. While the specific details of what it does are classified, the Service welcomes general inquiries on issues of national security. Its publications offer extensive information for the general reader:

- An annual Public Report discusses Canada's security environment and the Service's national security role.
- An occasional publication, *Commentary*, carries essays on longer-term strategic topics involving national security, based on unclassified information.
- *Perspectives* is a series of unclassified papers written by the Research, Analysis and Production Branch, focusing on current issues of concern to the Service.
- *Backgrounders* are issued periodically on national security issues.

These documents and other material are available on the CSIS Web site (**www.csis-scrs.gc.ca**).

The Service also responds to media and other inquiries, and reaches out to the general public by sending representatives to speak at various community, academic and corporate functions.

The Numbers

The CSIS Web site attracts increasing numbers of visitors wishing to learn about national security issues and the role played by the Service. The site offers a wide range of information, from guidance on how to apply for employment with CSIS to backgrounders on national security issues.

CSIS Web Site Statistics, 2004-2005	
Total number of Web site requests for menu pages and documents:	1,943,476
Web site requests for CSIS publications:	
Commentary	198,830
Perspectives	109,852
Backgrounder No. 8: *Counter-Terrorism*	44,562
Anti-Globalization—A Spreading Phenomenon, Report No. 2000/08, *Perspectives*	22,844
Chemical and Biological Terrorism	8,539
Most frequently visited Web pages:	
Recruitment information and job postings	212,541

CSIS Access to Information Statistics
April 1, 2004, to March 31, 2005

Type of requests	Number received	Number dealt with during 2004-05	Number outstanding at end of 2004-05
Privacy requests	353	332	21
Access requests	98	90	8
Totals	**451**	**422**	**29**

Maximizing Our Resources

Human Resources

"I have come away … with a very favourable impression of the competence, dedication and commitment of Service employees at all levels and at the varying lengths of service. Most of all I have been struck by the integrity with which the organization and its staff meet its mandate; its workforce is one of its greatest assets."

—Extract from the Inspector General's Certificate, November 2004

Recruiting and Training

CSIS has an extremely capable workforce, thanks to rigorous recruitment and continuous learning. A large number of employees have impressive qualifications.

In response to increased operational demands, in 2004-2005 the Service recruited additional subject-matter experts and intelligence officers. Subject-matter experts are recruited sometimes for intelligence officer positions and sometimes for other positions within the Service.

The Service employs scientists, linguists, academic specialists, program engineers and other highly trained technical specialists. Most new intelligence officers are recruited from the ranks of recent university graduates. Successful candidates come from a variety of academic backgrounds. Ideally, but not necessarily, candidates are fluent in more than one language, and have had international travel exposure and/or exposure to different cultures. The Service's workforce has capabilities in 86 languages and 34 percent of intelligence officers can speak a language other than English or French.

After joining the Service, intelligence officers must undergo training and acquire experience before they become fully operational.

A Diverse Workforce and a Respectful Workplace

CSIS prides itself on being an equal opportunity employer with a diverse workforce that is increasingly representative of Canadian society. Diversity is also essential for the Service to be able to effectively meet the challenges of today's threat environment.

CSIS actively recruits members from under-represented groups and strives to make the recruitment process fair. For example, the Service's psychologists ensure that psychological tests and interviews are not culturally biased. The intelligence officer profile is reviewed annually; subsequently, psychologists update interview questions to reflect the profile and prevent discrimination in the overall assessment process.

The Numbers

CSIS Diversity Statistics

Employees who self-identified as belonging to a visible minority:	9.9 %
Intelligence officers who self-identified as belonging to a visible minority:	8.2 %
CSIS employees who were women:	47.7 %
Intelligence officers who were women:	39.5 %

The Service also strives to ensure that staff are respectful of diversity and sensitive to all cultures. Employment equity presentations and cultural awareness sessions form part of the Orientation Course for new employees, the Intelligence Officer Entry Training course and other development courses.

In addition, intelligence officers receive ongoing training in cultural awareness and sensitization.

Promoting Official Languages

The Service continues to be vigilant and proactive in meeting its official languages obligations under the *Official Languages Act*. Today, the first official language of 38 percent of CSIS employees is French. The Service offers language training to those who need it before they start their formal intelligence officer training; they must be bilingual before they take up an intelligence officer position.

Financial Resources

The Service's financial resources have increased starting in 2001-2002, as a result of greater funding for public safety and anti-terrorism allocated in the December 2001 federal budget. In addition, the Service has received funding for operational requirements related to marine security and the Smart Border Declaration.

In fiscal year 2005-2006, the CSIS budget will increase as a result of the inclusion of Employee Benefit Plan in the Service's budget. Other technical program adjustments are related to new and enhanced programs under the National Security Policy, announced in 2004.

Figure 1: Human Resources

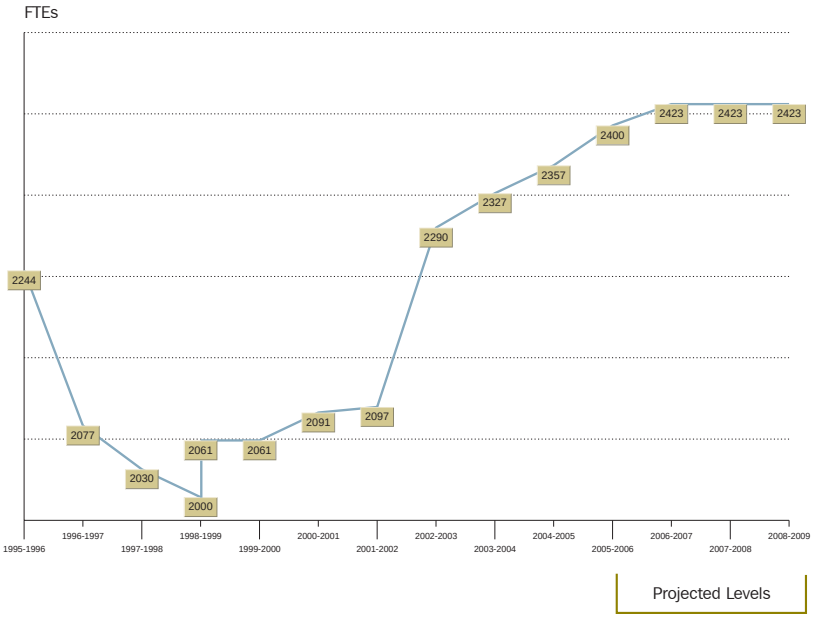

Figure 2: Financial Resources