2004

Report of the

# Auditor General of Canada

to the House of Commons

MARCH

## Chapter 3

National Security in Canada—
The 2001 Anti-Terrorism Initiative

Office of the Auditor General of Canada

*The March 2004 Report of the Auditor General of Canada comprises seven chapters, a Message from the Auditor General, and Main Points. The main table of contents is found at the end of this publication.*

The Report is available on our Web site at www.oag-bvg.gc.ca.

For copies of the Report or other Office of the Auditor General publications, contact

Office of the Auditor General of Canada
240 Sparks Street, Stop 10-1
Ottawa, Ontario
K1A 0G6

Telephone: (613) 952-0213, ext. 5000, or 1-888-761-5953
Fax: (613) 954-0696
E-mail: distribution@oag-bvg.gc.ca

*Ce document est également disponible en français.*


Cat. No. FA1-2004/1-3E
ISBN 0-662-36243-8

Chapter

# 3

## National Security in Canada

The 2001 Anti-Terrorism Initiative

*All of the audit work in this chapter was conducted in accordance with the standards for assurance engagements set by the Canadian Institute of Chartered Accountants. While the Office adopts these standards as the minimum requirement for our audits, we also draw upon the standards and practices of other disciplines.*

# Table of Contents

# National Security in Canada
## The 2001 Anti-Terrorism Initiative

## Main Points

**3.1** In response to the September 11 terrorist attacks on the United States in 2001, the Canadian government took several steps: It established the Ad Hoc Cabinet Committee on Public Security and Anti-Terrorism, chaired by the Deputy Prime Minister; mobilized the military, the RCMP, and the public service to manage the initial crisis; and then developed a long-range initiative to improve Canadian security. In the 2001 Budget, the government allocated $7.7 billion in new funds to be spent over the next five years on the Public Security and Anti-Terrorism initiative to enhance security for Canadians.

**3.2** Our audit examined the overall management of the Public Security and Anti-Terrorism initiative. We also examined the co-ordination of intelligence among departments and agencies and their ability to provide adequate information to enforcement personnel. In addition, we examined selected issues in greater detail—the interoperability of security and intelligence information systems; fingerprint identification; and the assessment of airport workers who require clearances to restricted areas. Other countries, including the United States, have examined similar areas and reported findings comparable with those of our audit.

**3.3** We found that the government had developed management systems to direct and control spending and reporting on activities under the initiative. The vast majority of funds allocated in the 2001 Budget have been channelled to priority areas. In addition, the Treasury Board Secretariat is tracking spending and attempting to assess the security improvements achieved by the initiative. However, we found that the government did not have a management framework that would guide investment, management, and development decisions and allow it to direct complementary actions in separate agencies or to make choices between conflicting priorities.

**3.4** The government as a whole failed to achieve improvements in the ability of security information systems to communicate with each other. Consequently, needed improvements will be delayed by several years. Moreover, even as the government was launching programs that would create new needs for fingerprint identification, projects that would have helped it to deal with the increased demand were not included in the initiative.

**3.5** We also found deficiencies in the way intelligence is managed across the government. A lack of co-ordination has led to gaps in intelligence coverage as well as duplication. The government as a whole did not adequately assess intelligence lessons learned from critical incidents such as September 11 or develop and follow up on improvement programs. Individual

agencies have created new co-ordinating mechanisms, but some departments are still not participating in them.

**3.6** We found gaps and inconsistencies in the watch lists used to screen visa applicants, refugee claimants, and travellers seeking to enter Canada. There is no overall quality control of this vital function, which is spread over several departments and agencies. No one monitors delays in the entry or the quality of the data on watch lists.

**3.7** Finally, criminal intelligence data are not used to screen applicants for clearance to restricted areas at airports, meaning that security clearances are issued without checking applicants for criminal association. Transport Canada is not provided with all the information available to police and therefore has issued restricted area clearances to many individuals whose reliability must be questioned. Unless air transportation workers with access to aircraft are reliable, spending on passenger and cargo security will be of reduced value.

**The departments and agencies have responded.** In general, they have agreed with our recommendations although commitments toward remedial action are sometimes vague. We found that the responses from the Canada Border Services Agency and Public Safety and Emergency Preparedness Canada provide a clear picture of their intentions.

# Introduction

## The impact of September 11

**3.8** On September 11, 2001 the United States suffered an unprecedented terrorist attack that destroyed the World Trade Center, damaged the Pentagon, destroyed four civilian airliners, and killed thousands of citizens. The immediate effects on Canada were the need to deal with the shutdown of civil air transport and look after passengers on grounded airliners; heightened border security; and a sudden sense of personal and economic insecurity.

**3.9** The crisis period lasted several months, during which the federal government had to sustain internal and border security operations at a high level. Defence, intelligence, police, and border control agencies worked to full capacity. Ministers and senior managers sought to deal with policy and budget issues on an urgent basis, while at the same time drafting emergency legislation and guiding it through Parliament.

**3.10** In the longer term, the federal government has had to develop policies and programs to deal with the threat of terrorism not only to Canada directly but also to the United States and the rest of the world.

**3.11** **Management of national security.** Unlike the United States—but similar to both the United Kingdom and Australia—Canada had not consolidated domestic security agencies under a single department until 12 December 2003. Instead, like its Commonwealth colleagues, it relied on Cabinet and co-ordinating agencies to manage security affairs. This audit assessed the situation prior to the 2003 reorganization.

**3.12** On 12 December 2003, the Prime Minister announced significant changes to the structure of parliamentary committees, departments, and agencies. The principal changes involving national security are the following:

- A new department, Public Safety and Emergency Preparedness Canada, has been created from the former Solicitor General Canada. The new department includes the Office of Critical Infrastructure Protection and Emergency Preparedness, transferred from National Defence.
- The Canada Border Services Agency, reporting to the Minister of Public Safety and Emergency Preparedness, comprises the Customs Branch from the former Canada Customs and Revenue Agency, the intelligence and enforcement sections from Citizenship and Immigration Canada, and the border inspection function of food, plant, and animal health from the Canadian Food Inspection Agency.
- The new position of National Security Advisor to the Prime Minister in the Privy Council Office will co-ordinate integrated threat assessments, help strengthen interagency co-operation, and assist in the development of an integrated policy framework for national security and emergencies.
- The Minister of Transport is now responsible for security in all transportation sectors.

- A new Cabinet Committee on Security, Public Health and Emergencies will manage national security and intelligence issues and activities and government-wide responses to public health, national disasters, and security emergencies. It will replace the Ad Hoc Committee on Public Security and Anti-Terrorism.

**3.13** At the time of our audit, the government delivered national security programs through many departments and agencies. In general, national security programs include national defence, policing and federal law enforcement, intelligence, border control, transportation security, critical asset protection, and disaster and emergency management. The principal organizations involved in program delivery are detailed in Exhibit 3.1.

**3.14** Until December 2003, no single minister below the Prime Minister was responsible for Canada's security. The organizations involved in security reported to their respective ministers, who were accountable for their activities. Ultimately the Prime Minister was, and remains, accountable for the security of the country and therefore provides broad guidance. The Prime Minister usually chaired the annual Meeting of Ministers on Security and Intelligence. Other Cabinet committees such as the Cabinet Committee on Social Union made decisions when security and intelligence involved broader social policy issues. The new organization consolidates many of these departments and agencies under a single minister.

**3.15** In late September 2001, the Prime Minister established the Ad Hoc Cabinet Committee on Public Security and Anti-Terrorism to review policies, legislation, regulations, and programs across the government in order to strengthen all aspects of Canada's approach to fighting terrorism and ensuring public security. The Chair of the Committee (the Deputy Prime Minister) was charged with co-ordinating overall elements of the government's response to the events of September 11. Members of the Committee were the Solicitor General and the ministers of Finance, National Defence, Transport, Foreign Affairs, Justice and Intergovernmental Affairs, National Revenue, Citizenship and Immigration, and Health.

**3.16** This ad hoc committee, like other ad hoc committees of Cabinet, was established to address time-sensitive issues that cut across the mandates of several ministers. The Committee provided advice to the Prime Minister and Cabinet and remained active in discussing national security issues and providing general policy direction, but it did not regularly make program or policy decisions. These were normally referred to permanent committees of Cabinet. The Ad Hoc Committee on Public Security and Anti-Terrorism continued to meet on a regular basis during our audit. It has now been replaced by the Cabinet Committee on Security, Public Health and Emergencies.

**3.17** Below the ministerial level, the Privy Council Office—the Prime Minister's "department"—co-ordinates bureaucratic efforts. The Clerk of the Privy Council chairs the Interdepartmental Committee on Security and Intelligence (ICSI), which includes the deputy heads of the main agencies involved and is the main executive forum that reviews major policy issues

**Exhibit 3.1 Principal organizations involved in national security program delivery, at the time of our audit***

| Organizations | Program delivery |
|---|---|
| **National Defence** | • provides defence of country |
| **Canadian Forces** | • deployed overseas to advance and protect Canadian values and interests<br>• responsible for JTF2, a high-readiness counter-terrorism unit that rescues hostages or undertakes other action required in response to a terrorist incident<br>• maintains a chemical-biological-nuclear company to respond to attacks against Canada |
| **Communications Security Establishment** | • collects and analyzes foreign signal intelligence<br>• helps ensure the federal government's own telecommunications are secure |
| **Office of Critical Infrastructure Protection and Emergency Preparedness** | • provides national leadership to protect Canada's physical and cyber infrastructure against threats (natural disaster or purposeful attack)<br>• ensures civil emergency preparedness |
| **Solicitor General Canada** | • oversees public safety and provides policy direction to its agencies<br>• responsible for the National Counter-Terrorism Plan, which outlines roles and responsibilities for managing terrorist incidents |
| **Royal Canadian Mounted Police** | • enforces federal laws as Canada's national police service<br>• provides contract policing to most provinces, the three northern territories, many municipalities, and First Nations communities<br>• provides forensic services and criminal intelligence to Canadian and foreign police<br>• responsible for primary investigation of criminal offences related to terrorism and espionage<br>• protects Governor General, Prime Minister, and visiting foreign dignitaries<br>• provides on-board security on selected civil airline flights |
| **Canadian Security Intelligence Service** | • investigates, analyzes, and advises government departments and agencies on potential threats to Canada's national security<br>• investigates political violence and terrorism, espionage and sabotage, and foreign-influenced activities detrimental to Canadian national interests, such as interference with ethnic communities in Canada<br>• provides security assessments for all federal government personnel requiring a security clearance (except the RCMP); transportation workers; and immigration, citizenship, and refugee applicants |
| **Foreign Affairs and International Trade** | • manages day-to-day conduct of relations with foreign states and peoples<br>• protects Canadians and Canadian government facilities abroad<br>• handles terrorism incidents abroad involving Canadians<br>• manages such issues as the expulsion of foreign diplomats from Canada for security reasons<br>• through its Security and Intelligence Bureau provides Minister with foreign intelligence to support policy and operational decisions and advises Minister on intelligence activities |

*On 12 December 2003, the Prime Minister announced significant changes to these organizations (see paragraph 3.12).

**Exhibit 3.1 Principal organizations involved in national security program delivery, at the time of our audit* (continued)**

| Organizations | Program delivery |
|---|---|
| **Financial Transactions and Reports Analysis Centre of Canada** | • receives, collects, and analyzes transaction reports, provided by financial institutions, financial intermediaries, the Canada Customs and Revenue Agency, and others<br>• discloses relevant information to law enforcement agencies, where appropriate<br>• *Anti-terrorism Act* required disclosure of information to CSIS where there are reasonable grounds to suspect it is relevant to a threat to the security of Canada |
| **Citizenship and Immigration Canada** | • ensures immigrants and visitors do not represent a risk<br>• deals with people-smuggling, organized crime, terrorism, war crimes, and crimes against humanity<br>• protects Canada as a border security agency |
| **Canada Customs and Revenue Agency** | • enforces border, tax, and trade laws and regulations<br>• protects Canada as a border security agency<br>• responsible for helping fulfill Canada's obligation regarding illegal export of nuclear, chemical and biological weapons or compounds |
| **Canadian Food Inspection Agency** | • delivers all federal food inspection, animal health, and plant protection measures<br>• protects Canada as a border security agency<br>• responds to biological outbreaks of pests and diseases in plants and animals |
| **Transport Canada** | • sets and enforces security standards for air, land, and water transportation systems<br>• evaluates information from the security and intelligence community<br>• directs the transportation industry to take appropriate action to deal with threats<br>• assists emergency response personnel in handling dangerous goods emergencies<br>• responsible for overall transportation security policy and regulations but relies on others, including marine and airport authorities, to ensure transportation system is secure |
| **Canadian Air Transport Security Authority** | • screens air transport passengers and their belongings prior to boarding<br>• screens checked baggage<br>• provides on-board security for selected flights under a contract with the RCMP<br>• provides federal financial support to local airport operators for airport policing related to aviation security |
| **Fisheries and Oceans Canada**<br>**Canadian Coast Guard** | • conducts dual-use maritime surveillance to enforce fishing regulations and to support other security operations<br>• provides control of vessel traffic |

*On 12 December 2003, the Prime Minister announced significant changes to these organizations (see paragraph 3.12).

**Exhibit 3.1 Principal organizations involved in national security program delivery, at the time of our audit* (continued)**

| Organizations | Program delivery |
|---|---|
| **Health Canada** | • operates Centre for Emergency Preparedness and Response, which co-ordinates public health security in Canada<br>• lead department on bio-terrorism, develops and maintains emergency response plans<br>• manages the Global Public Health Intelligence Network, which identifies disease outbreaks around the world<br>• manages the National Emergency Services Stockpile system, which includes pharmaceuticals necessary to treat people exposed to biological agents<br>• maintains equipment and supplies for 165 "field hospitals" with 200 beds each<br>• operates the National Microbiology Lab, Canada's first Level 4 lab<br>• lead department for the Federal Nuclear Emergency Plan |
| **Natural Resources Canada** | • regulates the security of energy pipelines through the National Energy Board, and explosives, nuclear energy, and materials through the Canadian Nuclear Safety Commission<br>• complies with its security regime for nuclear facilities and other nuclear activities including armed response at power stations against penetration |

*On 12 December 2003, the Prime Minister announced significant changes to these organizations (see paragraph 3.12).

Source: *The Canadian Security and Intelligence Community*, Government of Canada, 2001, and other information from departments and agencies.

before they are considered by ministers. The Deputy Clerk, Counsel and Security and Intelligence Co-ordinator chairs the ICSI Executive Subcommittee composed of deputy ministers of the core intelligence agencies and the Department of Justice. (Deputy ministers would also meet before each meeting of the Ad Hoc Cabinet Committee on Public Security and Anti-Terrorism.) Finally, an Intelligence Policy Group of officials at the assistant deputy minister rank is chaired by the Assistant Secretary of the Security and Intelligence Secretariat, Privy Council Office. These committees have been left in place.

**3.18** Solicitor General Canada was responsible for maintaining the National Counter-Terrorism Plan, which outlines roles and responsibilities for managing the response to incidents of terrorism. The Senior Assistant Deputy Solicitor General chaired the Assistant Deputy Minister Committee on Public Safety, which shared many members with the Intelligence Policy Group. The Committee on Public Safety provided a co-ordination and discussion forum for policy and priority setting in law enforcement and public safety. Solicitor General Canada, with the participation of the Treasury Board Secretariat, is leading an initiative to improve information sharing on public safety and security. The department has been renamed Public Safety and Emergency Preparedness Canada and expanded to include border services and emergency preparedness.

**3.19** **New funding.** During October 2001, the government approved several major new allocations of funds, including

- $30 million annually to provide immediate, permanent staff increases to the Canada Customs and Revenue Agency, Citizenship and Immigration Canada, the RCMP, and Transport Canada;
- $250 million for immediate security initiatives—largely capital and equipment—to 15 departments and agencies;
- $71.5 million in urgent funding to offset unforeseen costs such as overtime for Customs and the RCMP; and
- $160 million to compensate Canadian air carriers and specialty operators for losses resulting from the closure of Canadian air space following the September 11 attacks.

**3.20** Except for the funds to compensate air carriers, these amounts were part of the $7.7 billion announced in the December 2001 Budget as new spending over 2001–02 and the following five years for enhanced security, emergency preparedness, and improving border infrastructure. The Budget was designed to keep Canada safe, keep terrorists out, and keep Canada's border open. It announced $6.5 billion for security, including the creation of a new air security authority, additional funding for intelligence and policing, and funding for Canada's military; and more than $1.2 billion for initiatives designed to make Canada's border more secure, open, and efficient.

**3.21** The Budget included major investments to

- equip and deploy more intelligence and front-line investigative personnel, improve co-ordination among agencies, and boost marine security ($1.6 billion);
- improve screening of immigrants, refugee claimants, and visitors (including detention and removal), speed up the determination of refugee claims, and introduce new fraud-resistant Permanent Resident Cards ($1 billion);
- improve the protection of critical infrastructure and emergency preparedness and response; and expand the military's anti-terrorism capacity ($1.6 billion);
- create a new air security organization, place armed plainclothes police officers on Canadian aircraft, purchase explosive-detection equipment, and enhance air transportation policing ($2.2 billion); and
- enhance border security and improve the infrastructure that supports major border crossings to ensure the legitimate flow of goods and people ($1.2 billion).

## Focus of the audit

**3.22** This chapter focusses on two overarching themes: the overall management of the Public Security and Anti-Terrorism initiative; and the co-ordination of intelligence among departments and agencies and their ability to provide adequate information to enforcement personnel.

It examines several specific issues—the interoperability of security and intelligence information systems and the sharing of information, fingerprint identification, the use of watch lists for border control, and the security clearance of airport workers requiring passes to restricted areas.

**3.23** We reported on the level of independent review of security and intelligence agencies in an audit observation included in the Auditor General's November 2003 Report, Chapter 10.

**3.24** Further, we plan to conduct an audit in the future that will focus on air travel security, elements of marine security, and consequence management.

**3.25** More details on the objectives, scope, approach, and criteria for the present audit are included at the end of the chapter under **About the Audit**.

## Observations and Recommendations

Planning and control of the initiative

### Management of the security initiative and review of departmental proposals

**3.26** The Ad Hoc Cabinet Committee on Public Security and Anti-Terrorism oversaw the plan for "Enhancing Security for Canadians," a $7.7 billion component of the December 2001 federal Budget. The Committee asked deputy ministers of 17 departments and agencies to submit proposals on how they could support five broad objectives for funding decisions:

- keep terrorists out of Canada;
- deter, prevent, detect, and prosecute and/or remove terrorists;
- facilitate Canada–U.S. relations;
- support international initiatives (such as the UN, NATO, NORAD); and
- protect our infrastructure and support emergency planning.

**3.27** This process was unusual in that the Privy Council Office took the lead, with support from the Treasury Board Secretariat and Finance Canada, to identify specific security measures in response to September 11. A three-agency committee (assistant deputy ministers from the Privy Council Office, Finance Canada, and the Treasury Board Secretariat, chaired by the Privy Council Office) reviewed the spending plans submitted by departments before making recommendations for inclusion in the Budget submission. Officials in departments told us the Privy Council Office had warned that it would be wary of "opportunism." Unless they were considered justified by the change in circumstances, certain items were ruled ineligible—such as reversals of Program Review cuts, unfunded Cabinet submissions, and measures to address the rust-out of equipment. There was an unwritten policy to apply the "user pay" principle wherever possible. Our examination of the process was limited primarily to interviews, as there were no formal minutes of discussions or recommendations and few documents recording discussions of proposals. Departments said they had found the review process rigorous and sometimes intimidating.

**3.28** Many departments already had long-range plans prepared that encompassed the desired enhancements; the December 2001 Budget provided an opportunity to implement and expand those plans. Examples are the Customs "Action Plan 2000–2004" and Citizenship and Immigration Canada's "Permanent Resident Card" project.

**3.29** Though the committee had recommended funds for allocation to departments based on their proposals, access to the funds was not automatic after the Budget was passed. Departments and agencies had to submit proposals for the Treasury Board's approval before they could obtain access to the funds.

**3.30** Some proposals were for substantially higher amounts initially than the amounts that were finally approved. Examples include proposals by Citizenship and Immigration Canada and the RCMP, whose final allocations were only about a third of their original requests.

**3.31** For the handful of projects that cut across a number of departmental lines, lead departments were identified to consolidate departments' separate proposals into one submission to the Treasury Board. For example, Transport Canada co-ordinated a combined submission on marine security; National Defence led an initiative to improve the response to chemical, biological, radiological, and nuclear emergencies.

**3.32** The lead departments were responsible for co-ordinating discussion among the supporting departments and, after reaching consensus, preparing a consolidated submission to the Treasury Board. In one case, the Office of Critical Infrastructure Protection and Emergency Preparedness allocated funds to sub-projects in the supporting departments.

### Most items selected for funding were directly connected to Budget objectives

**3.33** We looked at the projects funded by the Public Security and Anti-Terrorism (PSAT) initiative and compared them with the stated objectives used in the review performed by the Privy Council Office, the Treasury Board Secretariat, and Finance Canada. The initiative's overall purposes as announced in the 2001 Budget were to keep Canadians safe, keep terrorists out, and keep the borders open. We found that the vast majority of items put forward by departments and reviewed by central agencies showed a direct connection to the stated objectives.

**3.34** In the Budget section "Enhancing Security for Canadians," a total of $510 million was allocated to National Defence to support Canada's military, including $210 million to fund Canada's international military campaign against terrorism. The remaining $300 million was allocated to defence activities other than anti-terrorism initiatives, including $69 million to develop a Joint Strike Fighter, $14.5 million to develop vaccines, and $2 million to support the cadet program.

**3.35** We found no evidence that officials of the Privy Council Office, Finance Canada, and the Treasury Board Secretariat had based their review of departmental proposals on a national threat and risk assessment. A framework based on such an assessment can help ensure that projects are

given the appropriate priority, taking into account alternative uses of the funds and potential levels of risk.

**3.36** Other projects appeared designed to maintain the government's existing public safety and policing programs, not to respond directly to the increased need for security after September 11. For example:

- The RCMP was allocated $45 million to replace an outdated occurrence management system. This is the system police use to record and store information on the bulk of their actions and investigations. After an earlier failed attempt to replace its existing system, the RCMP received approval under the initiative to acquire and implement a replacement. Funding for most of the new system's expected costs was allocated in the 2001 Budget.
- Of the $250 million in emergency funding, the Canada Public Safety Information Network was allocated $3.75 million, with an additional $4.75 million annually beginning in 2002–03. This network, managed by Solicitor General Canada, comprises many initiatives designed to improve information sharing throughout the justice system by linking criminal justice agencies with other agencies across the country, leading to increased public safety.
- Public Security and Anti-Terrorism funds were allocated to the Solicitor General to combat organized crime and the illegal drug trade in First Nations communities, including the cultivation of marijuana. This project was allocated $300,000 in 2001–02 and $1.5 million annually in ongoing funding beginning in 2002–03.

**3.37** At the same time, certain proposed projects that appeared directly related to the Budget objectives were not funded fully. These included marine security and the RCMP's Real Time Identification system. We were told by officials that certain projects had not been developed well enough to be considered for funding at the time of the Budget. Marine security was addressed after the original Budget allocations, but the Real Time Identification system has not yet been funded. We could not look further at these decisions because the review process followed by Finance Canada, the Treasury Board Secretariat, and the Privy Council Office was not fully documented.

**3.38** Certain other projects fall into a grey area. While they show a vague link to combatting terrorism and supporting the objectives of the Budget, these are not their main activities. For example:

- The RCMP was allocated over $5 million to replace an outdated laboratory information management system that tracks laboratory casework.
- The concept of Integrated Border Enforcement Teams (IBETs) predates the Budget, but their implementation was accelerated as a result of increased funding. The teams are designed to protect the Canadian/U.S. border at places other than ports of entry. The teams share intelligence and investigate and interdict persons and organizations that pose a threat to national security or are suspected of criminal activity. Teams

include representatives of Canadian and U.S. police and border enforcement agencies. While the vast majority of their work focusses on contraband and illegal immigrants, their investigations may provide valuable intelligence and develop into a national security investigation.

### Funds from the initiative are subject to additional controls

**3.39** **Restrictions on reallocation within departments.** When increased resources are approved for departments by the Treasury Board, they are most often combined with other departmental resources and are subject to the standard policies and regulations that govern spending by departments. Departments and agencies are free to reallocate their resources among programs as their needs and priorities change. However, they were not to reallocate PSAT funds for other purposes without notifying the Treasury Board and assuring it that their PSAT activities would not be affected. In certain cases, access to PSAT funds was further restricted by separating PSAT expenditures from other departmental transactions.

**3.40** In most cases, departments accepted the allocation of funds as provided. In other cases, departments subsequently provided further information. For example, marine security, a horizontal project involving seven departments and agencies, was initially allocated $60 million in the 2001 Budget. After approximately $25 million of this amount was allocated to specific projects, the departments provided threat assessments that were more detailed, and the allocation was increased in January 2003 by $172.5 million to a total of $197.5 million.

**3.41** Citizenship and Immigration Canada believed that reallocating the funds it had received would provide better results toward the Public Security and Anti-Terrorism objectives. It presented an alternative allocation among its projects, which the Treasury Board approved in August 2002. The emphasis was on building an intelligence capacity and improving screening to better identify and remove security risks. This is in contrast to the RCMP, who did not press for funding of the Real Time Identification system even though it underpinned the success of other projects. This is discussed in detail later in the chapter.

**3.42** **Requirement to report on PSAT results.** In addition to restricting the use of Public Security and Anti-Terrorism funds to projects related to the initiative's objectives, the Treasury Board imposed a framework on departments and agencies for reporting on and evaluating their project results. This was the first attempt we had noted by central agencies to monitor the spending and results of an initiative across departmental and agency lines. We were told that this reporting requirement would not only serve to monitor progress but also provide a means for the Treasury Board to reallocate funds from certain projects to others with higher priority.

**3.43** The first annual reports were due on 30 September 2003. The deadline was missed by most departments although a large number subsequently filed their reports. Therefore, it is too early to determine whether this approach to monitoring results will work. The documents that we did receive varied widely in the amount of detail on actions taken and results achieved. The

Treasury Board Secretariat needs to improve this process as a basis for central direction and better accountability to Cabinet and parliamentary committees.

**3.44** It is not clear that the reporting framework will provide the information needed to oversee the initiative. Much of the funding was allocated not to establish new programs but to increase the capacity of existing programs. Consequently, while departments and agencies can estimate the amounts they have spent, it will be difficult to separate the results of the initiative's activities from those of ongoing departmental programs.

**3.45** The 2003 Budget announced that the Treasury Board Secretariat would lead a series of reviews of departmental and horizontal programs. The government chose Public Security and Anti-Terrorism as one of the horizontal reviews, currently under way.

**3.46** **Recommendation.** The Treasury Board Secretariat should ensure that departments and agencies with projects funded under the Public Security and Anti-Terrorism initiative complete their annual reports and detail the specific results of their projects to the appropriate committees of Cabinet and Parliament.

**Treasury Board Secretariat's response.** Agreed. The majority of departments and agencies have met the requirement to report on their Public Security and Anti-Terrorism initiatives for the previous year's activities, and for future years. The Secretariat is analyzing the information and will be reporting to the Treasury Board on the results. As well, the Secretariat intends to provide departments and agencies with direction by May 2004 on reporting requirements to Parliament.

## Management of security intelligence

**3.47** Intelligence is a product of the collection, evaluation, analysis, integration, and interpretation of all available information. Security intelligence is used to warn the government about activities that may threaten Canada's security. It is one of the most effective tools available for enforcement programs and border protection, both of which are key priorities of the government's Public Security and Anti-Terrorism initiative. Intelligence information is also needed so limited resources can be focussed selectively and precisely on the greatest threats.

The Canadian Security Intelligence Service (CSIS) National Headquarters. CSIS, along with the other organizations mentioned in this chapter, contributes to Canada's security.

### Gaps in management hinder progress

**3.48** The importance of intelligence in the fight against terrorism cannot be overstated. Co-ordinating the efforts of the agencies involved is acknowledged as critical to their overall effectiveness. After September 11, many departments recognized that their intelligence function needed strengthening. This was especially the case for Immigration, which created a new intelligence branch and, in March 2002, initiated a major reorganization of its intelligence function.

**3.49** At the time of our audit, overall direction came from five high-level government committees that co-ordinate activities within the intelligence community. However, committees co-ordinated the activities of autonomous agencies only when there was consensus. When agencies could not reach consensus or discussions dragged on too long, they needed direction from an executive authority. Our examination showed that opportunities exist to improve co-operation and integration; to resolve disputes among organizations; and to learn from past events.

**3.50** We believe that executive authority and direction based on and derived from an accountability framework are key to addressing these issues.

### Better co-operation and integration are essential

**3.51** The challenges of responding to threats of terrorism have made it clear that co-operation and integration are important tools. The government appears to be moving in the right direction, with efforts to more closely co-ordinate the collection of intelligence information and to encourage the exchange of information among analysts.

**3.52** We expected to see the intelligence community co-operating to produce and disseminate intelligence reports efficiently. We also expected to see formal mechanisms established and controlled to co-ordinate the activities of the community, particularly analysis and distribution of intelligence.

**3.53** Intelligence priorities of individual agencies are collected by the Privy Council Office, which analyzes them and draws common themes that are then presented to ministers for their endorsement at the annual Meeting of Ministers on Security and Intelligence. As these deliberations are a category of Cabinet confidences to which we do not have access, we were unable to assess this process.

**3.54** **Strategic intelligence.** Strategic intelligence is based on the in-depth analysis of a threat and is a mix of open and classified material. Its purpose can be to inform policy makers or to provide background to investigators, analysts, and enforcement officials. Two principal groups produce strategic reports: the Intelligence Assessment Secretariat in the Privy Council Office and the Research, Analysis and Production Branch in the Canadian Security Intelligence Service. We were told that the Intelligence Assessment Secretariat focusses on international intelligence while the Research, Analysis and Production Branch focusses on specific threats to Canada. Users

of these reports told us they had received the reports in a timely manner and in most cases had found them useful.

**3.55** However, in some cases the distinction between the two areas of focus is not easy to discern, based on the similarities we saw in a number of reports from both organizations. The Privy Council Office told us that similar reports can help in ensuring that different perspectives and viewpoints inform policy making.

**3.56** **Tactical intelligence.** Tactical intelligence is more urgent, warning of an imminent threat or a potentially illegal act. When intelligence agencies learn of an imminent threat to a specific person or event, they can alert enforcement agencies.

**3.57** We expected to see that tactical reports or alerts reached enforcement staff promptly, and in most cases we found this to be so. However, we found that the communication of alerts can rely on personal contacts and informal networks. In one case, an alert to a potential threat was sent using the government's top secret messaging system but was addressed incorrectly. After waiting a month for a response, the sending agency followed up and found that the message had not been received. Fortunately, the alert turned out to be a false alarm.

**3.58** In another case, an alert from an ally did not reach the departmental intelligence unit it was intended for because the Canadian agency that initially received it had sent it to an emergency centre, which failed to circulate it.

**3.59** We also noted that the Office of Critical Infrastructure Protection and Emergency Preparedness has only limited access to the government's top secret messaging system. For urgent alerts it depends on the telephone and facsimile transmission.

**3.60** **New efforts at integrating activities.** In response to the attacks of September 11, agencies in the security and intelligence community recognized the importance of integrating their activities. Information on known or suspected terrorists and on potential threats, vulnerabilities, and previous events exists in many forms and in many places. Assembling this information is the challenge facing the community.

**3.61** We noted a number of examples that illustrate the need for central co-ordination. The RCMP's projects under the Public Security and Anti-Terrorism initiative included the creation of Integrated Border Enforcement Teams (IBETs) and the Integrated National Security Enforcement Teams (INSETs). Each incorporates members of other agencies and in some cases other levels of government and the United States. The concept is recognized as a good one, and the RCMP's annual report on PSAT funding has noted some successes. However, we noted that not all of the intelligence agencies participate fully in these integrated teams. Notable is the lack of full participation in the INSETs by Citizenship and Immigration Canada and its lack of members on the IBETs. Immigration officials told us that they support

the IBETs initiative but decided against full participation at the present time as, in their view, the primary focus of IBETs is on drugs and contraband.

**3.62** In early 2003, the Canadian Security Intelligence Service created the Integrated National Security Assessment Centre (INSAC) and outlined its purpose in a framework document. The Service envisioned a centre that would use intelligence from many sources to produce timely analyses and assessments of threats to Canada and would distribute these reports to those with national security or public safety responsibilities. It invited the following organizations to send a representative:

- Canada Customs and Revenue Agency
- Communications Security Establishment
- National Defence
- Office of Critical Infrastructure Protection and Emergency Preparedness
- RCMP
- Transport Canada
- Department of Foreign Affairs and International Trade
- Citizenship and Immigration Canada
- Solicitor General Canada
- Privy Council Office

The latter four organizations have not yet provided a representative. Foreign Affairs said that its resources should more properly address the threat to its personnel and assets abroad and that increasingly scarce resources from a 'foreign ministry' should not be devoted to matters that are better left to domestic agencies. Immigration told us it supports the concept and attributes its absence to the lack of permanent funding available for that purpose. Solicitor General Canada said that although it has not assigned a specific representative, its officials are fully engaged in all functions and work initiated by the Centre. The Privy Council Office told us that it has no intelligence collection mandate but is actively involved on a daily basis in the processing of information produced by INSAC.

**3.63** Documents we reviewed show that the Canadian Security Intelligence Service created INSAC because it recognized the importance of sharing information. The concept of establishing an integrated assessment centre was endorsed by the Intelligence Policy Group. However, at the time of our audit INSAC still did not have a mandate that had been agreed to formally by all the parties. We also note that it will be less effective if four organizations in the intelligence community fail to participate fully.

**3.64** While integrated units represent an improvement, in each case they were initiated by a single agency; we are concerned that participation by other departments and agencies is discretionary. We are also concerned that without an accepted framework to guide their development, such groups could proliferate and lead to duplication.

**3.65** **Resolving issues among organizations.** We found cases where mandate or co-operation issues among organizations have remained unresolved for a considerable time. Specifically, we found the following:

- The potential for the activities of the RCMP and the Canadian Security Intelligence Service to overlap has increased since the *Anti-terrorism Act* was passed. Both organizations have undertaken new ways of working together, through INSETs and mutual secondments and collaboration in the scientific and technical fields. Notwithstanding that their working relationship is critical and they see it as progressing well, their memorandum of understanding covering joint work and co-operation has not been updated to reflect their revised responsibilities.
- In another case, we noted an unresolved issue between two organizations involving the use of intelligence in an investigation.

**3.66** In our opinion, the most significant issue still unresolved is Customs officials' lack of access at the front line to information on lost and stolen passports (discussed in greater detail later in this chapter).

**3.67** We noted that privacy concerns were often cited as the reasons why agencies could not exchange information. However, officials were not able to show us any legal opinions, specific references to legislation, or judgments as a basis for that position.

**3.68** **Recommendation.** The National Security Advisor should consider the following when developing a planned integrated policy framework:

- a common understanding of domestic security;
- defined roles, responsibilities, and accountabilities; and
- clear goals and objectives based on assessments of risks, threats, and vulnerabilities.

**Privy Council Office's response.** Agreed.

### Intelligence lessons learned from critical incidents are incomplete

**3.69** It is unreasonable to expect that the government can gather sufficient intelligence to protect Canada from all attacks. What is reasonable to expect is that after any significant incident, an organization will analyze how it responded, identify the lessons it learned, and apply those lessons in the future.

**3.70** **Learning from Ressam.** On 14 December 1999 a Montreal resident, Ahmed Ressam, was caught attempting to smuggle explosives into the United States from Canada. The Assistant Deputy Minister Committee on Public Safety commissioned a lessons-learned study that looked at operational deficiencies in the handling of the case and at vulnerabilities in the system. However, the Committee had no authority to direct departments to correct the problems or deficiencies that the study identified.

**3.71** The lessons-learned report (30 August 2001) noted that a number of the identified problems had been fixed but that several significant issues remained unresolved. The report was based on separate lessons-learned

reports submitted by individual departments and agencies. However, some agencies had not produced reports. For example, we found that while the Passport Office was significantly involved in the Ressam affair, it did not conduct a lessons-learned analysis.

**3.72** **Post-September-11 analysis.** We expected also to see a lessons-learned study that assessed how the Government of Canada had responded to the attacks in the United States. We found a wide variety of reports. In some cases, extensive analyses were carried out but never endorsed by senior management; lack of support by senior management undermines any effort to implement change. In other cases we were given basic reports that appeared to be summaries but that provided no detailed analysis (Exhibit 3.2).

**3.73** The Assistant Deputy Minister Committee on Public Safety produced an overall report that included a large section on assessments by provincial and territorial governments. The Committee produced an action plan and a status report in fall 2002. However, we found no reporting of progress made against the recommendations since that date.

**Exhibit 3.2** **Assessment of lessons-learned reports**

| Department or agency | Lessons-learned report | | Executive approval | Action plan | Status reports |
|---|---|---|---|---|---|
| | Summary | Internal report | | | |
| Privy Council Office | ✓ | | | | |
| Solicitor General Canada | ✓ | ✓ | | ✓ | ✓ |
| Canadian Security Intelligence Service | ✓ | | | | |
| Royal Canadian Mounted Police | ✓ | | | ✓ | |
| Office of Critical Infrastructure Protection and Emergency Preparedness | | ✓ | | ✓ | |
| Citizenship and Immigration Canada | ✓ | | | ✓ | |
| National Defence | | ✓ | ✓ | ✓ | |
| Transport Canada | | ✓ | | ✓ | |
| Canada Customs and Revenue Agency | | ✓ | | ✓ | |
| Communications Security Establishment | ✓ | | | ✓ | |

**3.74** The Interdepartmental Committee on Security and Intelligence proposed that heads of agencies meet with the Clerk of the Privy Council to provide a high-level perspective on the government's response to September 11. We noted that a four-page discussion paper prepared for that meeting was the only government-wide post-mortem analysis conducted. The heads of the RCMP, the Canadian Security Intelligence Service, and Finance Canada were not present at the dinner meeting held to discuss the paper. No record of the discussion was kept and no follow-up or action plan resulted.

**3.75** We were told that a presentation was made to the annual Meeting of Ministers on Security and Intelligence but that no minutes were kept and no action plan was produced.

**3.76** **Recommendation.** The National Security Advisor, with Public Safety and Emergency Preparedness Canada, should carry out a government-wide lessons-learned analysis after any significant security incident. Such an analysis should include an action plan that addresses the deficiencies identified and regular follow-up to assess progress.

**Privy Council Office's response.** Agreed.

**Public Safety and Emergency Preparedness Canada's response.** The Counter-Terrorism Operational Readiness section of the National Security Directorate has an informal lessons-learned process in place, which is incorporated in the development of scenario-based exercises, seminars, and workshops. Additionally, Public Safety and Emergency Preparedness Canada is amending its national response structure to capture lessons learned from operations and to incorporate these lessons into operational procedures. The formalized version of this lessons-learned process will address deficiencies and conduct regular progress assessments.

## Interoperability and information sharing

### Problems with the interoperability of information systems

**3.77** **A priority after September 11.** The government identified the interoperability of security information systems and the sharing of information as high priorities after September 11. The goal of interoperability was to make sure that those who needed information for their operations could get it and use it. The federal government knew that there were information "stovepipes" among federal departments and agencies and other levels of government. These barriers could prevent the timely recognition of threats to Canada and delay its response to terrorists or other emergencies, or make its response less effective.

**Dimensions of interoperability**

**Technical**—Systems applications transferring information

**Semantic**—Standardization of terminology and definitions

**Human**—The cultural willingness of organizations to share information

**Inter-community**—Pursuing partnerships and common solutions across departmental or jurisdictional barriers

**Legal**—The legal framework that allows sharing of information

Source: Interoperability Working Group and Treasury Board Secretariat

**3.78** **Problems in this area contribute to other deficiencies noted.** Elsewhere in this chapter we discuss problems that could be defined as a lack of interoperability or of information sharing:

- Watch lists require the timely sharing and transfer of information between those who collect the information and the Customs officers on the front line who use it in protecting Canada's borders.
- Information on lost and stolen passports needs to be available to officials on the front line.

- The increased reliance on intelligence requires a more effective and efficient means of sharing information among intelligence agencies.
- Officials screening people who work in secure areas of airports require more complete information from police to make informed decisions.

**3.79** **Assistant deputy minister working group problems.** In October 2001 the government formed the Interoperability Working Group, comprising assistant deputy ministers of departments and agencies with security and intelligence responsibilities. The group's objectives were to identify opportunities to enhance public safety, establish a list of "quick hits" (fixes) and medium-term initiatives to be pursued immediately, and propose a long-term vision and strategy to harmonize processes and improve information sharing.

**3.80** Departments and agencies began to work on some of the "quick hits" immediately after the working group identified its list in February 2002. The working group made a presentation to the Ad Hoc Cabinet Committee on Public Security and Anti-Terrorism in June 2002. The Chair of the working group approved an interim report in September 2002, but it was never submitted to Cabinet.

**3.81** The working group ceased to exist after June 2002, and we found no evidence to show that central direction had reassigned its responsibilities elsewhere. In November 2003, Solicitor General Canada was asked by the government to lead a program development initiative to improve the sharing of information for public safety and security, with the participation of the Treasury Board Secretariat. Given the priority of the issues involved and the potential impact on public safety and the security of Canadians, this delay points to a lack of central direction.

**3.82** Solicitor General Canada led a study of how information was shared at Pearson International Airport. The study found that information sharing often relied more on established personal relationships than on operational procedures or integrated electronic information systems. In some cases, guidelines restricted the sharing of information among departments. There were duplicate entries and duplicate searches among different departmental databases. There was a lack of co-ordination among agencies, which could hamper investigations. There were gaps in the information available for determining whether airport employees should be granted or should retain their security clearance. We made similar observations in the course of our audit.

**3.83** **Slow progress on "quick hits."** We found that progress on the quick hits identified by the Interoperability Working Group has not been sustained. In fact, in some areas where progress was reported it has since deteriorated. Only three projects have been completed successfully—for example, the provision of information on lost and stolen licence plates to our land border ports of entry; two have made doubtful progress; and five have made no progress since September 2002—for example, front-line officers at airports still do not receive passport information.

**3.84** **Recommendation.** Departments responsible for "quick hits" and other issues related to interoperability and information sharing should speed up efforts to resolve identified problems. The Treasury Board Secretariat and Public Safety and Emergency Preparedness Canada should monitor those efforts.

**Treasury Board Secretariat's response.** The Secretariat agrees that it will ensure the monitoring of these initiatives for sustained progress and expected results.

**Public Safety and Emergency Preparedness Canada's response.** The Department agrees with this recommendation and currently monitors the effective and appropriate implementation of the "quick hits" and other desired connectivities, as identified by post 9/11 working groups and others.

The "Public Safety and Security Information Sharing and Interoperability" project will consolidate these "hits" with other known gaps and ensure that public safety and security connectivities are prioritized and pursued as appropriate. Public Safety and Emergency Preparedness Canada and the Treasury Board Secretariat will work collaboratively to ensure that departments and agencies who are implementing these new connections receive support in co-ordinating their work with other agencies, in addressing any emerging Government of Canada public policy issues; and in obtaining any needed funding.

### Other issues not addressed by the Interoperability Working Group

**3.85** One initiative with significant interoperability requirements is Advance Passenger Information and the Passenger Name Record (API/PNR). Legislation passed in fall 2001 requires airlines to provide the government with API/PNR information in order that Customs and Immigration staff can identify and assess the risks presented by travellers before they arrive in Canada. Airlines collect API data when passengers check in; PNR is drawn from airline flight reservations systems and includes itinerary and method of payment. The effectiveness of this initiative depends on the databases of a large number of organizations other than the airlines, including Customs, Immigration, Taxation, RCMP, CSIS, and agencies in the United States.

**3.86** In October 2002, government departments began to collect API data. There were problems in obtaining data from one major airline, but these have been resolved. Progress is being made on PNR but it is slow, due in part to technical issues that must be overcome with each airline. Another obstacle is that airlines in the European Union have been prevented from providing data due to privacy concerns. In partnership with the United States, Canada has been developing an automatic evaluation of risks posed by arriving passengers. The two countries plan to share information on passengers whose risk scores exceed a pre-determined threshold.

**3.87** Another significant weakness is the absence of a government-wide system that would allow communication at the "secret" level among departments and agencies. A project undertaken by one agency was abandoned when the proposed methodology was found to be vulnerable to

attack. In November 2003, the government undertook to renew the development of a communications system at the secret level to complement the existing system for communication at the top-secret level.

**3.88** **Recommendation.** Public Safety and Emergency Preparedness Canada and the National Security Advisor, with the assistance of the Treasury Board Secretariat, should co-ordinate and oversee the implementation of a government-wide communications system at the secret level.

**Public Safety and Emergency Preparedness Canada's response.** The Department recognizes and supports the need for a government-wide communications system at the secret level and continues to support the planning and pursuit of related funding strategies for such an initiative, which will form part of the "Public Safety and Security Information Sharing and Interoperability" project.

**Privy Council Office's response.** Agreed that there should be a government-wide capacity to share secret information.

**Treasury Board Secretariat's response.** The Secretariat will assist Public Safety and Emergency Preparedness Canada and the National Security Advisor in ensuring that the communications system adheres to government-wide security and privacy policies.

### Priorities not yet identified

**3.89** At the time of this writing, the government had just brought forward a proposal to develop a plan for the sharing of public safety and security information. This plan will not deal with specific issues or individual information systems but will identify priorities and provide a framework to develop solutions. Developing such a plan was part of the longer-term vision of the Interoperability Working Group. Over the next two years, the plan will involve all departments and agencies with police, enforcement, legal, and intelligence responsibilities in the criminal justice and national security communities. Government officials recognize that this work has been delayed too long.

**3.90** The scope of the plan is very broad—it calls for examining the relationships among agencies and their hundreds of information systems, repositories of data, and the processes they support. It will not absorb or direct the ongoing development and implementation of projects now under way. However, it will attempt to link these projects, some of which involve development costs in the hundreds of millions of dollars, to allow for better sharing of information.

**3.91** The planning project is led by Public Safety and Emergency Preparedness Canada (formerly Solicitor General Canada), assisted by Canada's Chief Information Officer in the Treasury Board Secretariat; it will cost more than $9 million. The Chief Information Officer will provide expertise in a large part of the project design and implementation.

**3.92** **Access/privacy concerns.** To protect the privacy of individuals, many of Canada's laws prevent the sharing of information within the government.

We found that in some situations, departmental officials would not share or examine the possibility of sharing information, based on the assumption that it would contravene the principles of the *Privacy Act*. However, the *Privacy Act* accommodates the sharing of information among federal government agencies in a variety of situations, including for reasons of national security. We believe that some decisions not to share information were made without a proper examination of potential security concerns.

**3.93** In some cases, those requesting information asked for access to complete information systems. While this raises a legitimate privacy concern, a simple solution could be to isolate the requested information and make it available outside the main system, still protecting the privacy of individuals.

**3.94** **Recommendation.** The Privy Council Office and Public Safety and Emergency Preparedness Canada, with the assistance of the Department of Justice Canada and the Treasury Board Secretariat, should further examine and provide guidance on the sharing of information among government departments and agencies while balancing privacy concerns with national security concerns.

**Privy Council Office's response.** Agreed that the Privy Council Office and the Department of Public Safety and Emergency Preparedness should ensure that such guidance is provided to departments and agencies through the responsible departments, namely the Treasury Board Secretariat and Justice Canada.

**Public Safety and Emergency Preparedness Canada's response.** The Department is very mindful of the privacy implications of any information sharing and is developing, in partnership with other federal agencies and departments and in keeping with Treasury Board Secretariat Information Management policies, a framework for managing information under the Canada Public Safety Information Network, which respects Canadian privacy legislation and the Charter of Rights and Freedoms and enables effective information sharing in support of public safety and security.

**Justice Canada's response.** Agreed. We look forward to providing our expertise to government agencies to assist in enhancing our national security.

**Treasury Board Secretariat's response.** The Secretariat will continue to provide policy guidance in the areas of information management, privacy, and security with respect to the sharing of information among government departments and agencies.

## Improving fingerprint identification

**3.95** **Cornerstone of security identification programs.** Fingerprints are the fundamental biometric identifier on which criminal and security identification rests. Without fingerprints it is difficult to distinguish between persons with the same name or physical appearance, and it is extremely difficult to detect someone using a false identity. Fingerprints are used to positively identify applicants for security clearances, visas, and refugee claims. Canada has a single, national fingerprint identification system run by the RCMP.

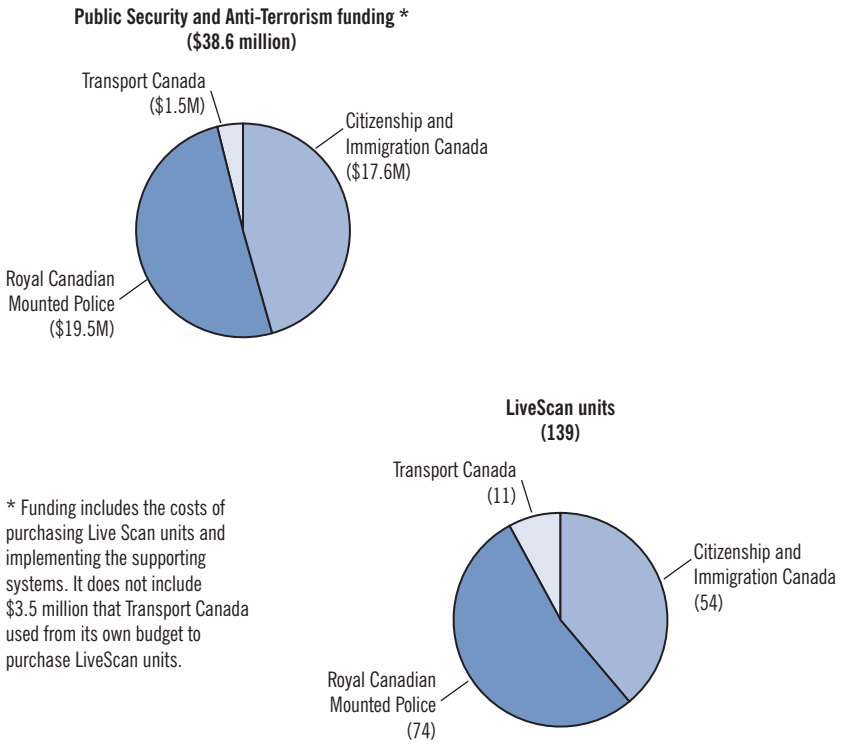
**3.96** Currently the fingerprint identification system has a fixed capacity, dependent on about 100 analysts. Training more analysts would take two years and would temporarily lower the production of experienced analysts, who would be needed to provide the training. Capacity can be significantly increased only by replacing the current analytical process with an automated one.

**3.97** The Public Security and Anti-Terrorism initiative included $38.6 million to improve the collection of fingerprints by using electronic LiveScan machines that take a digitized image. The funds were allocated to Citizenship and Immigration Canada, Transport Canada, and the RCMP (Exhibit 3.3). In the case of Transport Canada, the funding was used to extend its existing automated fingerprint identification initiative.

**3.98** **LiveScan was seen as a major initiative for fighting terrorism and increasing security at ports of entry.** LiveScan is an automated process for taking fingerprints, palm prints, and photographs of selected individuals. Fingerprints are transmitted electronically to the RCMP. Upon receipt, these prints are manually searched against the RCMP's national database, which contains 3.3 million sets of fingerprints including those of refugees and of criminals.

**3.99** In 2001, Citizenship and Immigration Canada, Transport Canada, and the RCMP purchased LiveScan equipment to modernize their fingerprinting

**Exhibit 3.3 Implementation of the LiveScan project**



An officer taking fingerprints using an automated LiveScan machine.

processes. Citizenship and Immigration Canada uses these machines to send prints of refugee claimants and inadmissible persons at ports of entry to the RCMP to verify their identity. Transport Canada uses them in determining whether to grant airport workers clearance to restricted areas. At Transport Canada's request, the RCMP runs the workers' fingerprints through the national database to see if they have a criminal record or are a risk to security. The Canadian Police Information Centre's database is also checked to see if the names match any active records in that system. The RCMP uses the national database to run checks on suspected criminals as well as public and private sector individuals who need a security check as a condition of employment.

**3.100** **Increased demand for fingerprint services.** The Forensic Identification Services branch of the RCMP is responsible for checking fingerprints against the national database. In the last two years, the branch has faced a growing demand to do more work with the same level of resources. For example, fingerprint analysis is now required in Canada Customs' Free and Secure Trade program and British Columbia's name change legislation; there are also more requests for checks of employees working in restricted areas.

## Business cases for LiveScan were inadequate

**3.101** There were 139 LiveScan machines purchased with Public Security and Anti-Terrorism funding. The cost of the machines and the planned expenditures on systems and maintenance until 2006–07 total $38.6 million. Transport Canada spent an additional $3.5 million from its own budget. We reviewed each of the business cases developed for the LiveScan project by Transport Canada, Citizenship and Immigration Canada, and the RCMP.

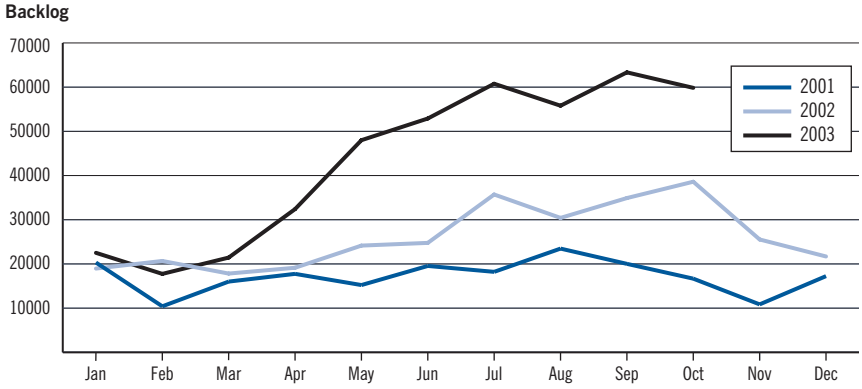
**3.102** We found that the business cases developed by Citizenship and Immigration Canada and the RCMP were inadequate. They did not provide enough information on the benefits of LiveScan; nor did they include an adequate framework for risk analysis. For instance, because the benefits of LiveScan were inextricably linked to the Real Time Identification system (RTID), which was needed to complete the automated process for analyzing fingerprints, we believe the business cases should have fully explored the fact that a failure to implement RTID posed a major risk to the success of LiveScan. In addition, these two business cases did not include an adequate options analysis. We could not tell whether there were options available for fingerprinting other than the system that was chosen.

**3.103** Transport Canada's business case met our criteria but based its estimate of benefits on the assumption that the RCMP would have RTID in place by the end of 2003. The RCMP did not receive the funds it would have needed to have RTID running by then. Benefits that Transport Canada estimated at $13 million have not been realized.

**3.104** **LiveScan did not improve turnaround times.** Each department claimed that LiveScan would reduce turnaround times for fingerprint analysis. However, our audit found that these benefits were marginal at best.

Fingerprints submitted for analysis have been of higher quality, leading to fewer rejects and improved accuracy. Although Transport Canada has processed four times more fingerprint files per month since the introduction of LiveScan, this is due not so much to the introduction of LiveScan as to additional RCMP personnel funded by Transport Canada and assigned to clearances for access to restricted areas at airports. Moreover, with the increase in demand for fingerprint analysis there has been a corresponding increase in the backlog of work. It would take over two and a half months to clear the backlog if no new requests for analysis were received. Therefore, while the turnaround times for Transport Canada's requests have clearly improved, the requests to the RCMP from other organizations have been added to the backlog (Exhibit 3.4).

**Exhibit 3.4 Backlog of fingerprints at the RCMP's Forensic Identification Services, 2001–2003**




Note: An average of 20,000 fingerprints are assessed each month.

**3.105** The RCMP developed a memorandum of understanding with Citizenship and Immigration Canada on turnaround times. Although the RCMP puts a high priority on processing the prints of suspected terrorists, the agreement establishes a turnaround time of six to eight weeks for most work requested by Citizenship and Immigration Canada. This is the same as the standard before LiveScan.

**3.106** The RCMP provided no information to show that LiveScan had improved turnaround times in its detachments.

**3.107 Recommendation.** The RCMP should find and implement a solution to deal with its fingerprint backlog.

**RCMP's response.** We agree with this recommendation. Indeed, the RCMP is committed to improving service delivery and has undertaken to secure funding for a long-term solution, a major project called Real Time Identification (RTID), for the full automated processing of fingerprints. In the interim, the RCMP is addressing the backlog by hiring additional employees, although these resources need to be supplemented due to the increasing demands. Both solutions, however, require funding not presently approved.

**Public Safety and Emergency Preparedness Canada's response.** The Department agrees that a solution to the fingerprint backlog is needed. The "Public Safety and Security Information Sharing and Interoperability" project will address interoperability pressures, including the need for modern fingerprint capabilities at the RCMP. In the interim, policy options for dealing with the backlog will be reviewed.

### LiveScan does not provide a fully automated system

**3.108** LiveScan takes fingerprints and transmits them in a digital format, but an outdated manual process is still used to analyze and compare them. The RCMP told us that it had proposed a central computerized system to analyze digitized fingerprints—the Real Time Identification system (RTID)—but had not received funding for it. Officials at the Treasury Board Secretariat explained that the RCMP's business case for RTID was not sufficiently developed to justify its funding. However, LiveScan without RTID will not achieve the efficiency levels estimated in the three separate business cases for LiveScan. The RCMP continues to seek funding for RTID. If it receives the funding it will still be three to four years before the RCMP sees the benefits that RTID promises for the fingerprinting process. If it does not obtain the funding, the benefits of electronic fingerprinting will take even longer to achieve.

**3.109** **Recommendation.** The RCMP and Public Safety and Emergency Preparedness Canada should give priority to implementing the Real Time Identification project.

**RCMP's response.** Agreed. In the wake of September 11, 2001, there was considerable public pressure to demonstrate responsiveness in a short period of time. This urgency was the context within which some decisions were not continually validated between agencies. The decision to support the deployment of LiveScan technology without supporting the critical fingerprint processing infrastructure was unfortunate. Funding needs to be allocated to this area as soon as possible.

**Public Safety and Emergency Preparedness Canada's response.** The Department agrees that implementation of the Real Time Identification project is a priority and continues to support the planning and pursuit of related funding strategies for this initiative, which will form part of the "Public Safety and Security Information Sharing and Interoperability" project.

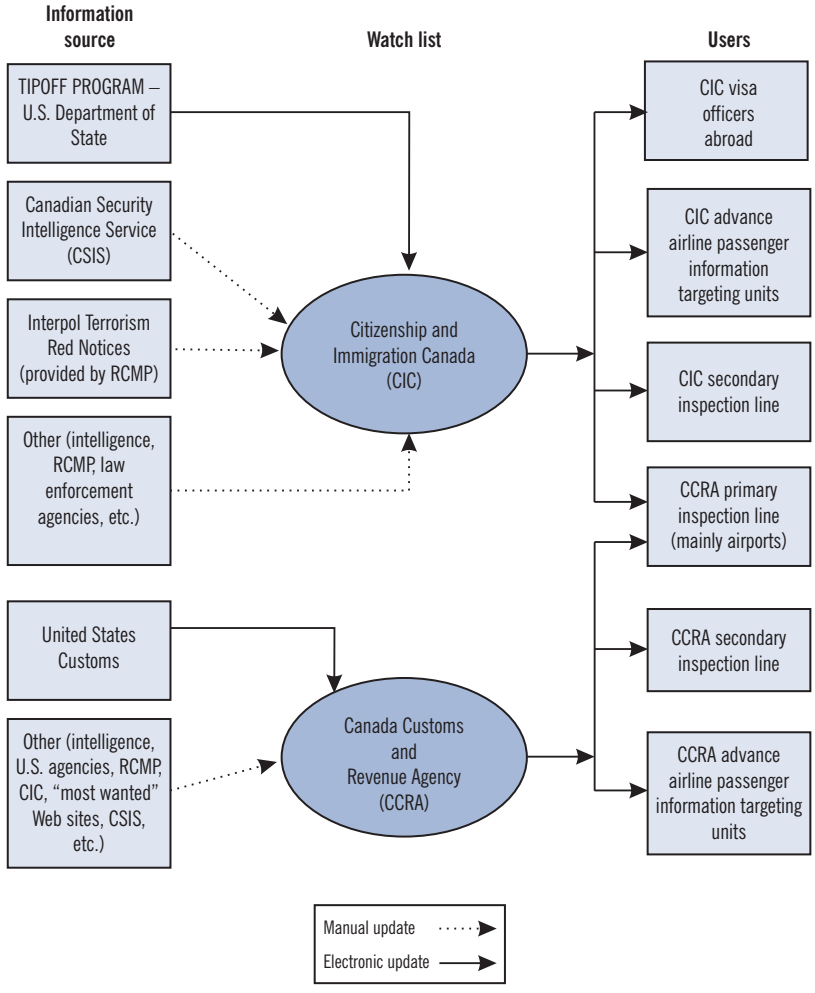
## Terrorist watch lists

**3.110** Watch lists play a critical role in ensuring our national security. They are a key tool in combatting terrorism by stopping terrorists before they reach Canada or by intercepting them at our ports of entry. Since September 11, the number of names on watch lists has grown dramatically. At Canada's airports, Customs officers on the primary inspection line check the names of arriving passengers against the watch lists. Watch lists are also used as an essential check in issuing visas, of which nearly 900,000 were issued in 2003.

**3.111** A small number of federal departments manage watch lists under a range of mandates that collectively contribute to national security. Citizenship and Immigration Canada and the Canada Customs and Revenue Agency are the primary users of watch lists for border control. The watch lists used by Immigration and Customs officials are derived from a small number of both foreign and domestic sources. Exhibit 3.5 provides an overview.

**3.112** The Canadian Security Intelligence Service provides Citizenship and Immigration Canada with "lookout" notices on persons it believes are inadmissible to Canada, including those who are believed to be a threat. These include known or suspected terrorists against whom the Service has enough information to support immigration inadmissibility proceedings as well as persons against whom it has less information but believes warrant close scrutiny.

**Exhibit 3.5 Border control watch lists**



**3.113** The Canadian Security Intelligence Service uses a manual, paper-based process to transfer new lookouts, modifications, and cancellations to Citizenship and Immigration Canada.


A traveller is screened at Customs' primary inspection line.

## Errors in terrorist watch lists

**3.114** In our initial audit work we found significantly fewer terrorist lookouts in the Service's tracking system than in Immigration's database, so we did a detailed comparison of the two lists. We found that Immigration's records were in such disarray that we were unable to complete a full reconciliation during the course of our audit. We found

- terrorist lookouts missing,
- extensive duplication of records within Immigration's database,
- classification errors that could result in inappropriate handling of individuals entering Canada, and
- names listed that should have been removed from Immigration's database.

**3.115** System and resource problems in the Canadian Security Intelligence Service can contribute to delays in putting names on watch lists. In one case, a known terrorist's name was approved for inclusion on a watch list but was not listed for over a year because the submission was lost in the Service's watch list computer system. Other listings were delayed because managers involved in the approval process were busy with other priorities. Also, some names were not reviewed regularly by the Service to determine whether they should remain on the watch lists, as it did not have a record of having placed the names on Immigration's watch list.

**3.116** We also found occasional administrative delays in the Service's co-ordinating unit and inputting delays at Citizenship and Immigration Canada. These delays mean that it can take days for approved additions to watch lists and weeks for modifications before they are reflected in Immigration's database. The Canadian Security Intelligence Service and Citizenship and Immigration Canada informed us that urgent changes are given priority, and our findings generally supported that assertion.

## Problems in updating watch lists

**3.117** Most additions to Canada's watch lists came from the United States government's TIPOFF program. It also provided the only automated feed into our border terrorism watch lists that adds, modifies, and deletes lookouts electronically.

**3.118** The TIPOFF terrorist watch list program served as a clearing house for sensitive information provided by both foreign and domestic agencies. At the time of our audit it contained about 100,000 name records of suspected terrorists, obtained mainly from the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency. The size of this database has grown significantly since September 11. Reports show that the

United States has also experienced difficulty in assembling unified and comprehensive watch lists from different organizations.

**3.119** At the time of our audit, Immigration's watch list contained 37,000 lookouts obtained from TIPOFF. Upon reviewing Immigration's records we found significant, sporadic breaks between updates otherwise obtained monthly from the U.S. State Department. Immigration told us that these delays were due to competing priorities, staffing problems, and certain technological issues. Specifically,

- there were no updates from the end of June 2003 to mid-October 2003. When Immigration's records were finally updated, the names of more than 8,000 suspected terrorists were added;
- there were no updates from November 2002 to May 2003. When Immigration finally updated its records, it added the names of over 5,000 suspected terrorists; and
- there were no updates from June 2001 to November 2001. When Immigration finally updated its records it added over 1,500 names. Those left off the list included two of the September 11 hijackers whom U.S. authorities had identified in August 2001.

**3.120** Although the data exchange between Immigration and TIPOFF is automated, names of suspected terrorists from TIPOFF are frequently rejected by Immigration's system due to incompatible coding. Those names do not make the watch lists until Immigration staff have reported the problems to the U.S. State Department. Any corrections would be included in the next update. In our review of reports on system-generated errors, we saw names that had been rejected and not corrected.

**3.121** **Interpol Red Notices.** Interpol Red Notices are used by member countries to seek the arrest and extradition of fugitives. Red Notices have been issued on some of the world's most dangerous organized crime and terrorist figures: in 1998 a Red Notice was issued on Osama Bin Laden. Interpol reported that in 2002 over 1,200 people were arrested world-wide, in part as a result of its Red Notices. In April 2001, the Canadian government began including Interpol Red Notices on Immigration's watch list to prevent international fugitives from entering Canada.

**3.122** The RCMP receives Interpol Red Notices, which are then provided to Immigration for addition to its watch list using a manual, paper-based process that is slow and prone to error. We conducted a number of tests and found the following:

- Immigration's records were incomplete. We examined a representative sample of Red Notices contained in Interpol's Terrorism Watch List, a classified subset of Red Notices. Based on the results, we estimate that Immigration's watch list is missing 8 percent of the wanted terrorists.
- Of the "recent" notices posted on Interpol's publicly available Web site, 27 percent were not on Immigration's watch list.

- Of the Red Notices for 2002 that Interpol had cancelled and that the RCMP subsequently removed from its database, 53 percent had not yet been removed from Immigration's watch list.
- Delays exist between the publication of Interpol Red Notices and their entry into the RCMP database, due to mailing time and backlogs at the RCMP. We looked at a random sample of 118 Red Notices published in 2003 and entered into the police database up to mid-July, 2003 (about a third of the total number). On average, 48 days elapsed from publication to entry in the police system. At the time of our testing, the RCMP had a backlog of 162 notices to be entered in its database that were two months old, on average.

**3.123** According to the RCMP, Interpol has introduced a new electronic system that a number of other countries are using and that provides Red Notice information on a timely basis. Although this system could significantly reduce the present delays, at the time of our audit the RCMP had no concrete plans to use it.

### Lost and stolen Canadian passports not on border control watch lists

**3.124** On average, more than 25,000 Canadian passports are reported lost or stolen each year. The RCMP believes that lost and stolen passports are a concern for our national security because of their potential use by terrorists or other criminals.

**3.125** Border watch lists do not contain the list of lost and stolen Canadian passports. In April 2003, the Passport Office instituted a policy that once a passport is reported lost or stolen, it is permanently deactivated. However, the information system used on the primary inspection line cannot distinguish between active and deactivated passports.

**3.126** Discussion of this issue among the Passport Office, Customs, and Immigration began in January 2003 and was ongoing at the time of this audit but had generated no solution or corrective action. We were told that privacy concerns had to be overcome before the Passport Office could share the list of lost and stolen passports with Citizenship and Immigration; then the list in the Customs primary inspection line system would be updated.

**3.127** Although information on lost and stolen passports is not on our border watch lists, it is entered into an RCMP database using a manual process that is paper-based, time-consuming, and prone to error. There are long delays between the reporting of a lost or stolen passport and the entering of the information into the RCMP database. We examined a representative sample of 97 entries made in the database during the 12 months ending August 2003. About 12 percent of those entries were abnormal, taking over 243 days; the rest of the sample took 70 days, on average.

**3.128** Most of the delays reflect how long it takes the Passport Office to send forms to the RCMP. Some of the more exceptional delays represent passport losses reported to Canada's missions abroad. Delays are compounded when

the RCMP rejects illegible handwritten forms and sends them back to the Passport Office for correction and resubmission.

**3.129** Although no backlog existed when our audit began, by the end of our audit the RCMP's data entry was one month behind and had a backlog of 4,032 forms waiting to be entered in its database on lost and stolen passports. The RCMP informed us that it is currently addressing the backlog.

**3.130** The Passport Office has its own database that includes lost or stolen passports, but it is not linked or reconciled with the RCMP's. At the time of our audit about 65,000 lost or stolen passports were recorded in the Passport Office's database. After we completed our audit, the RCMP and the Passport Office informed us that they had reached an agreement in principle for the Passport Office to enter information on lost and stolen passports directly into the RCMP's database.

### Outstanding warrants for serious criminal offences not all on watch lists

**3.131** On 24 September 2003, the RCMP database contained about 162,000 outstanding Canada-wide arrest warrants for serious criminal offences (not including immigration warrants). There is no system that transfers information on outstanding warrants to the border watch lists; although Immigration and Customs manually check names, this is not done at the primary inspection line. This means that the automatic computer checks at the primary inspection lines and computer checks made against passenger lists in advance of international flights cannot flag persons wanted under Canada-wide warrants. Customs may enter lookouts on fugitives manually when specific information is provided by police or found during periodic scans of most-wanted lists on the Internet.

**3.132** After we completed our audit, Customs informed us that it would be implementing a system that incorporates warrants contained in the RCMP database into information provided to officers on the primary inspection line. This will be provided only at airports as land ports of entry focus on licence plates rather than the names of individuals.

**3.133** **Recommendation.** The RCMP, the Canadian Security Intelligence Service, the Canada Border Services Agency, and the Passport Office should improve their management and co-ordination of watch-listing efforts that collectively contribute to Canada's national security.

**RCMP's response.** Agreed. The RCMP is actively working with all partners to improve both the reliability and timeliness of data going to watch lists and the dissemination of the intelligence.

**Canadian Security Intelligence Service's response.** Agreed. The Service recognizes that the Auditor General is making overall conclusions in relation to the security and intelligence community into which our programs feed. The Service exerts rigorous control in its management of entries into the watch list, in monitoring entries in-house, and in providing quality control by examining each case against CIC's legislative criteria before processing, and will continue to do so.

**Canada Border Services Agency's response.** CBSA agrees to the recommendation and will continue to work with our partners to improve the management and co-ordination of watch-lists.

The CBSA (Customs and Immigration Intelligence) has recently established the National Risk Assessment Centre (NRAC) to serve as the focal point for managing and co-ordinating national and international watch lists.

A pilot project is being planned with the RCMP to have direct access to the RCMP Interpol database that will allow daily access to new Interpol notices.

**Foreign Affairs and International Trade's response.** Agreed. We have developed a memorandum of understanding with Citizenship and Immigration Canada (to be transferred to the Canada Border Services Agency) for the sharing of data at the Primary Inspection Line (PIL).

**3.134** **Recommendation.** The RCMP, the Canadian Security Intelligence Service, the Canada Border Services Agency, and the Passport Office should improve the reliability of watch lists by enhancing quality control over the exchange of data to ensure that information is complete, accurate, and timely.

**RCMP's response.** Agreed. The Canadian Police Information Centre (CPIC) Advisory Committee, comprising representatives of all CPIC partners, is now considering a proposal to move to Interpol's Automated Electronic Automated Search Facility system. If approved, this will significantly increase the speed of dissemination.

**Canadian Security Intelligence Service's response.** Agreed. The Service remains committed to working with lead agencies on interoperability, which would improve the program from a point of view of reliability and timeliness, thus ensuring better accuracy. The Service, which is fully automated internally, is inhibited from electronically interfacing with the recipients due to their inability to receive information in that format.

**Canada Border Services Agency's response.** CBSA agrees to the recommendation and will continue to work with our partners to improve the reliability of watch lists.

The exchange of data is already improving, as the Passport Office list of lost and stolen passports will be available to CBSA officials at the ports of entry by the summer of 2004.

Another significant achievement to be realized in the short term relates to automated searches for outstanding warrants, which are contained in the Canadian Police Information Centre (CPIC) database. Under the API/PNR program, CBSA currently targets high-risk air passengers and checks for warrants associated with these passengers through CPIC. By spring 2005, all air passengers' names (and eventually all sea passengers') will be searched against CPIC for outstanding warrants prior to their arrival in Canada.

Additionally, a quality assurance project was put in place in September 2003 to manually review all watch lists available to front-line staff and to address exception reporting. The project will be completed by March 2004.

In the medium term (within the next three years), technological improvements will permit all watch lists (terrorism, criminal, and lost and stolen passports) to be automatically updated via an electronic link between the originating holders of information and the new Global Case Management System shared by CBSA and Citizenship and Immigration Canada.

**Foreign Affairs and International Trade's response.** Agreed. The transfer of responsibility from the RCMP to the Passport Office for data entry of lost and stolen passports into the Canadian Police Information Centre (CPIC) database will reduce the handling of information and the risk of duplication, and it will improve the timeliness and integrity of the data.

## Security clearances for airport workers

### Improving air transport security was a major objective

**3.135** One of the major objectives of the 2001 Budget was to improve security at Canada's airports. According to the Budget document, "Rigorous new national standards for security in airports and on board flights are essential to protecting people. This budget will therefore provide Transport Canada with funds to strengthen its capacity to set regulations, review standards, and monitor and inspect all air security services."

**3.136** The Budget allocated $2.2 billion over five years to fund improvements that included

- creating the Canadian Air Transport Security Authority to be responsible for passenger and baggage screening and contributing towards policing at airports. The RCMP is responsible for placing armed police on flights;
- hardening aircraft cockpit doors to prevent the takeover of the flight deck by hijackers; and
- tightening access to aircraft by strengthening security zones at handling facilities and on airport tarmacs.

**3.137** The Budget did not specifically allocate funds to improve the security screening of airport workers with "air side" access—that is, those working in controlled-access areas of the airport where baggage and freight are handled and aircraft are serviced. If workers in secure zones are unreliable, many of the other improvements will be ineffective.

**3.138** Over 110,000 workers in Canada's airports have access to the "air side." Transport Canada screens each worker to eliminate persons who are known or suspected to be involved in threats of violence against persons or property, who are known or suspected to be members of an organization involved in violence or "closely associated" with such a person, or who the Minister of Transport reasonably believes might be prone to interfering with civil aviation.

**3.139** Transport Canada screens each applicant for an air side clearance by checking for

- a criminal record,
- terrorist links, and
- unreasonable indebtedness.

**3.140** Transport Canada performs credit checks on its own and relies on the RCMP to check for criminal records, the Canadian Security Intelligence Service to check for terrorist links, and on Customs to determine whether the applicant has had any Customs violations. While the Canadian Security Intelligence Service provides information based on a complete biography of individuals, the RCMP provides only information on whether a person has been charged or convicted of a criminal offence—information that does not identify for Transport Canada whether a person has associations with organized crime or is a refugee claimant. Based on the information it receives, Transport Canada determines whether a security clearance should be issued.

**3.141** We reviewed the systems and procedures used by the RCMP and the Canadian Security Intelligence Service for the extent of their screening procedures, timeliness of service, and cost.

**3.142** We audited the RCMP's and Customs' active investigation files for five major Canadian international airports (at Halifax, Montréal, Toronto, Calgary, and Vancouver). We also selected a sample of 405 restricted area clearance holders and asked the RCMP to determine whether any of them had significant criminal associations that might warrant a review of their clearance. We thank the RCMP for undertaking this work on our behalf; its knowledge and access to these systems provided for a more efficient examination.

### Criminal associations are a significant threat to air transport security

**3.143** **Increasing level of criminality.** Transport Canada exercises considerable discretion in the granting of clearances to restricted areas at airports. A criminal record may be the outcome of some offence unlikely to reoccur or to pose a threat to air transport. Individuals with a record of such an offence may be given a security clearance.

**3.144** We examined persons holding clearances at five Canadian Airports—Toronto, Montréal, Vancouver, Halifax, and Winnipeg—and found that about 3.5 percent have criminal records. In the general population, 9 percent of Canadians have criminal records. However, based on our analysis about 5.5 percent of clearance holders hired between January 2001 and May 2003 had criminal records. While this is still lower than the Canadian average, the upward trend over the last two years is of concern.

**3.145** Transport Canada officials told us that the clearance program focussed on a relatively narrow concept of "unlawful interference with civil aviation," which concentrated on the risks of hijacking and sabotage. This concept has been derived from international conventions. The risks of drug smuggling and other criminal activity were not necessarily regarded as grounds for denial of a clearance.

**3.146** **Number of active investigations.** The Canada Customs and Revenue Agency and the RCMP both investigate criminal conspiracies at Canadian airports; generally these involve drug smuggling. We reviewed the investigation files at the five airports we visited. Police and Customs had identified 247 individuals with clearances to restricted areas who were

involved in criminal conspiracies, almost all of them in Toronto and Montréal with a few in Vancouver (no such individuals were identified at the airports in Halifax and Calgary). Customs and police officials consider that even a small percentage of clearance holders with criminal intent poses a serious threat. A single criminal may bribe or coerce entire work teams to facilitate smuggling. Those involved rarely know what is being smuggled.

**3.147** The RCMP's assessment of clearance holders indicates a greater problem than is indicated in the criminal conspiracy investigation files at airports. At the two airports where police and Customs had no active investigations, clearance holders included individuals who may have significant criminal associations.

**3.148** **Extent of criminal association.** Each of the 405 individuals in our sample was assessed for criminal association by the RCMP's Criminal Intelligence Directorate, based on its information in three databases—the Canadian Police Information Centre, the Police Information Retrieval System, and the National Criminal Databank. We asked the RCMP if its intelligence files indicated any associations that might preclude the issuing of a clearance to a restricted area. Such associations would include, for example, membership in a biker gang, a spouse or close relative involved in organized crime, or an address associated with criminal activity. It is important to note that such individuals would not necessarily have a criminal record themselves or be active in organized crime; we also note that none of the 405 clearance holders in our sample had been assessed by Transport Canada for criminal association.

**3.149** Based on the results of the RCMP's database search on the 405 persons in our sample (generalized to the total number of people holding clearances to restricted areas at the five airports), we estimate that about 4,500 persons or 5.5 percent have possible criminal associations that warrant further investigation and possibly withdrawal of some security clearances. This represents a serious threat to security at airports.

**3.150** In addition to identifying individuals with criminal associations, the RCMP identified 16 businesses operating at airports that were linked to criminal activity such as providing travel arrangements for organized crime, facilitating identity fraud, and selling stolen passes. The firms were associated with biker gangs, organized crime, and drug trafficking. No firms with terrorist associations were discovered. At the two airports where Customs and the RCMP had no active criminal conspiracy investigations, nine companies with criminal links were operating.

**3.151** **Recommendation.** Where there is sufficient evidence, the Canada Border Services Agency should support the RCMP in conducting criminal conspiracy investigations at the two airports that had no active cases at the time of our audit.

**Canada Border Service Agency's response.** CBSA continues to work with our partners to investigate any criminal conspiracy at airports where there is

sufficient evidence identified by law enforcement to support such an investigation.

**RCMP's response.** The RCMP continually assesses the extent of criminal associations and the existence of criminal conspiracies in the course of our business. This is being done at all airports, including the two that did not have current investigations at the time of the audit. Where the RCMP does not have primary jurisdiction of the airport, the assessments are done in conjunction with the police service of primary jurisdiction.

### There are no legal barriers to strengthening airport security

**3.152** During our audit, various officials told us that there were legal barriers to wider sharing of criminal intelligence information. For example, some mentioned that individuals had a Charter right to freedom of association that precluded denial of a security clearance.

**3.153** In our opinion, there are no legal barriers to sharing police data with Transport Canada. However, police and Transport officials may have to assess the trade-off between revealing to an individual that the police have a file on him or her and safeguarding the security of air transportation.

**3.154** **Recommendation.** The RCMP and Transport Canada should reconsider the sharing of police intelligence information on criminal associations of applicants for and holders of clearances to restricted areas at airports.

**RCMP's response.** Agreed. The RCMP is actively consulting with Transport Canada and examining current processes to identify and address gaps or vulnerabilities in the current process of sharing information and intelligence.

**Transport Canada's response.** Both Transport Canada and the RCMP recognize the importance of sharing police intelligence information on criminal associations of applicants for, and holders of, clearances to restricted areas at airports. Moreover, effective February 16, 2004, the Government of Canada added another layer of security to the nation's aviation system by unveiling a new program to screen non-passengers who are authorized to enter restricted areas at Canada's major airports. Under the program, non-passengers—such as airline personnel, airport employees, refuelers, flight crews, caterers, aircraft groomers, maintenance personnel and ground handlers—are subject to random screening when accessing restricted areas at major airports.

Transport Canada is committed to working with the RCMP and other police forces to help facilitate and improve the sharing of information, while respecting privacy concerns.

**3.155** **Recommendation.** Once it has obtained access to complete police information, Transport Canada should begin a comprehensive review of all clearance holders.

**Transport Canada's response.** Currently, Transport Canada is of the opinion that it is bound by the *Aeronautics Act*, which restricts the scope of the

regulations to "preventing unlawful interference with civil aviation" (ss 4.7(2)). The clearance program has focussed on the "unlawful interference with civil aviation" concept (hijacking, sabotage, etc.) derived from international conventions. The risks of drug smuggling and other criminal activity are not necessarily regarded as grounds for denial of a clearance.

The proposed *Public Safety Act* (Bill C-7) would strengthen, clarify, and expand authorities relating to security clearances for transportation workers.

Transport Canada's analysis would suggest that the number of persons with criminal associations who should have their security clearances withdrawn is very small. Should it prove necessary, with the new system that supports the Transportation Security Clearance program, it will be possible for these persons to have their clearances removed in an accelerated manner.

Transport Canada is developing options for implementing a comprehensive review and will also be determining what is needed to achieve it.

## Conclusion

**3.156** The current management framework of the Public Security and Anti-Terrorism initiative met most of our audit criteria. The vast majority of funds allocated in the 2001 Budget have been channelled to identified priority areas. In addition, the Treasury Board Secretariat is taking care to track spending and is attempting to assess the improvements achieved by the initiative.

**3.157** Nevertheless, the management framework failed to ensure improvement in the ability of security information systems to communicate with each other. Consequently, needed improvements have been delayed by several years. Moreover, even as the government was purchasing equipment to digitize the collection of fingerprints and launching programs that would create new demands for fingerprint identification, projects that would have helped it to deal with the increased demand were not included in the initiative.

**3.158** We also found deficiencies in the management of intelligence. At the top level, we did not find a strategic framework guiding investment in and development of intelligence information. The government as a whole did not produce adequate lessons-learned assessments of critical incidents such as the September 11 attacks, nor did it develop and follow up on improvement programs. Some agencies have created new co-ordinating mechanisms, but some departments are still not participating in them.

**3.159** Watch lists used to screen visa applicants, refugee claimants, and travellers seeking to enter Canada are in disarray. There is no overall quality control of this vital function, which is spread over several departments and agencies. No one monitors delays in entering data or the quality of the information.

**3.160** Finally, we found that applicants for clearance to restricted airport areas are not being checked against available intelligence databases. As a result, restricted area clearances are granted to many individuals whose reliability must be questioned. Unless air transportation workers with access to aircraft are reliable, spending for the security of passengers and cargo will be of reduced value.

**3.161** Overall, these gaps and deficiencies point to a requirement to strengthen the management framework for security and intelligence. Improvement is especially needed in the management of issues that cross agency boundaries, such as information systems, watch lists, and personnel screening.

# About the Audit

## Objectives

The objectives of the audit were to

- determine whether the management framework for the Public Security and Anti-Terrorism initiative was adequate to ensure that funding decisions reduced risks to Canadians by the maximum extent possible;
- determine whether intelligence services work efficiently together and provide enforcement personnel with adequate information; and
- determine whether air transportation workers are adequately screened for reliability in a timely manner.

## Scope and approach

The scope of the audit included the overall management of the Public Security and Anti-Terrorism initiative, intelligence and information management, and reliability screening for airport restricted area clearances. The audit included all departments and agencies that support the PSAT initiative, but focussed on the Privy Council Office, the Treasury Board Secretariat, Solicitor General Canada, the Canadian Security Intelligence Service, the RCMP, National Defence (including the Communications Security Establishment), the Canada Customs and Revenue Agency, Transport Canada, Citizenship and Immigration Canada, and the Department of Foreign Affairs and International Trade.

We undertook the audit by interviewing headquarters staff of those organizations, reviewing files and records, sampling databases, reviewing audit trails for electronic records, and visiting operational sites such as airports, marine ports, and intelligence offices. We also visited selected officials in the United States and Australia.

## Criteria

Our audit was based on the following criteria:

- Funding should be allocated according to an overall intelligence-based threat assessment and a sound appreciation of existing security capabilities.
- Departments'/agencies' progress and performance documents should provide a good basis for co-ordinating and controlling the PSAT initiative.
- Departments should track and report costs related to the PSAT initiative.
- The government should employ appropriate management systems and practices to implement the PSAT initiative in a cost-effective manner.
- Accountability should be defined to resolve disputes in a timely manner, eliminate overlap and duplication, and result in integrated approaches to the production of intelligence.
- Intelligence resources should be allocated consistently and on the basis of a risk assessment.
- Intelligence reports and alerts should reach front-line staff in a timely manner.
- Security and intelligence staff should have systematically assessed the September 11 attacks and other important incidents and improved their capabilities.
- Officials should not unduly withhold information from other agencies when doing so would impair security.
- Transport Canada should be aware of any criminal associations of airport workers granted Restricted Area Access Clearance and other transportation workers granted similar clearances.
- Transport Canada should be able to demonstrate due diligence in its consideration of applicants with incomplete CSIS checks.
- There should be time standards for clearances, established by the needs of the transportation sector.
- CSIS should be resourced to meet response standards.

## Audit team

Assistant Auditor General: Hugh McRoberts
Senior Principal: Peter Kasurak
Principal: Gordon Stock
Directors: Dan Thompson, Edward Wood

Darren Canning
Dawn-Alee Fowler
Carol McCalla
Paul Pilon
Harold White

For information, please contact Communications at (613) 995-3708 or 1-888-761-5953 (toll-free).

# Report of the Auditor General of Canada to the House of Commons—March 2004

## Main Table of Contents