2009

Status Report
of the Auditor General of Canada to the House of Commons

Chapter 1
National Security:
Intelligence and Information Sharing

Office of the Auditor General of Canada

The 2009 Status Report of the Auditor General of Canada comprises a Message from the Auditor General of Canada, Main Points—Chapters 1 to 5, an appendix, and five chapters. The main table of contents for the Report is found at the end of this publication.

The Report is available on our website 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: 613-943-5485
Hearing impaired only TTY: 613-954-8042
Email: distribution@oag-bvg.gc.ca

Ce document est également publié en français.

Cat. No. FA1-2009/1-1E
ISBN 978-1-100-11824-6

Chapter

1

National Security: Intelligence and Information Sharing

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: Intelligence and Information Sharing

Main Points

What we examined

Security intelligence is the collection, evaluation, analysis, integration, and interpretation of all information used to warn a government about activities that may threaten a country's security. In Canada, the intelligence community consists of several organizations within the federal government, some of which collect information while others use it to deliver their programs or enforce the law. Because of the intrusive powers of agencies and departments involved in intelligence gathering and law enforcement, there are also organizations that review and publicly report their findings on the activities of these security and intelligence agencies.

In 2003, we reported that independent reviews of security and intelligence agencies and their reporting to Parliament varied significantly among agencies. In 2004, we reported that intelligence management across the government was deficient in many areas, from setting priorities for intelligence to coordinating and sharing information between departments and agencies. We also found deficiencies in the assessment of lessons learned following critical incidents, information and communications systems, watch lists, and personnel screening in airports.

For this status report, we examined the progress made since 2004 by 14 departments and agencies in their management and sharing of intelligence information, including the interoperability of their systems to support information sharing.

We also examined three review organizations—the Security Intelligence Review Committee (SIRC), the Commission for Public Complaints against the RCMP, and the Communications Security Establishment Commissioner—to assess the progress made by the government in response to our 2003 recommendation that security and intelligence agencies be subject to levels of external review and reporting that is proportionate to their level of intrusion into the privacy of individuals.

Why it's important

Tragic events such as the Air India disaster in 1985 and the September 2001 terrorist attacks in New York and Washington—and the more recent convictions of individuals in connection with terrorism-related offences—demonstrate the need for effective security intelligence by government organizations. More recently, Justice Dennis O'Connor's reports on the events relating to Maher Arar, as well as the proceedings of the Senate Special Committee and the House of Commons sub-committee on the *Anti-terrorism Act*, have underlined the need for better intelligence and information sharing between departments and agencies in Canada. The need for adequate management of intelligence activities is even more important in light of the challenges to security posed by events such as G-8 summit meetings and the upcoming 2010 Olympics in Vancouver.

For Canadians to have confidence in their security and intelligence organizations, they need to know that government agencies and departments maintain a balance between protecting the privacy of citizens and ensuring national security. Canadians also need to have confidence that the decisions and activities of intelligence agencies are legal, consistent, and appropriate, and that they are subject to examination by independent review agencies for reporting to their minister or Parliament.

What we found

- The federal government has made satisfactory progress since our 2003 and 2004 audits in implementing our selected recommendations for managing security intelligence. It has taken a number of initiatives to respond to our findings. We found progress in the organization and coordination of priorities among federal departments and agencies involved in security. The government also reduced the fingerprint backlog and is progressing in its development of a computerized system to analyze digitized fingerprints. It also took measures to improve the reliability of watch lists of individuals considered to be of interest to intelligence organizations. In other areas, there was either little or no progress or it was slow.

- Transport Canada and the Royal Canadian Mounted Police (RCMP) are still not sharing criminal intelligence information effectively. While Transport Canada has implemented additional procedures, the process does not access all data in the RCMP information management systems. In addition, the memorandum of understanding between the RCMP and Transport Canada regarding information sharing was terminated by the RCMP on 31 December 2007 as it no longer complied with ministerial direction or with the recommendations of the Commission of Inquiry into the

Actions of Canadian Officials in Relation to Maher Arar. Transport Canada may still be allowing high-risk individuals with criminal links to be cleared for access to restricted areas at airports.

- Since our 2003 audit, the government has assessed the level of review to which security and intelligence agencies are subject, and it is considering options for the future. However, at the time of this audit, the extent of independent review was still disproportionate to the level of intrusion these agencies may have into people's lives. As illustrated in recent testimony and reports by commissions of inquiry, the situation remains unchanged since our 2003 audit.
- We noted 16 cases, some reported more than once, where departments and agencies have reported legal barriers to information sharing. The Department of Justice Canada has not completed its research on how to manage the balance between the legal requirements for protecting the privacy of individuals and those for maintaining the security of the nation. As we also noted in our 2004 chapter, this has led to poor sharing of information among government departments. Progress, if any, has been slow since our 2004 audit.
- The development of a government-wide communications system at the secret level has progressed to the stage of limited implementation. However, it is over budget and behind schedule. While the system's future success depends on whether additional funding is obtained and whether its targeted users will adopt it, Public Safety Canada and the Treasury Board of Canada Secretariat remain confident.

The Government has responded. The departments and agencies agree with our recommendations. Their detailed responses follow each recommendation throughout the chapter.

Introduction

1.1 In Canada, a number of federal organizations are part of the intelligence community. 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.

1.2 Departments and agencies are involved to varying degrees in the collection of security intelligence, with varying levels of intrusion into people's lives. In some cases, information is gathered through covert means such as surveillance and wiretaps. In other instances, the information is gathered using public sources such as the media or by compulsory reporting of financial transactions to the government. The actions of some of these departments and agencies are subject to review by other offices.

What we found in previous audits

1.3 In November 2003, we reported that independent reviews of security and intelligence agencies and their reporting to Parliament varied significantly among agencies. For example, the Canadian Security Intelligence Service (CSIS) is reviewed by two bodies external to CSIS—the Inspector General and the Security Intelligence Review Committee—while the Royal Canadian Mounted Police (RCMP) is subject to more limited review. The current levels of review of security and intelligence agencies are shown in Exhibit 1.1.

1.4 In March 2004, as part of a broader examination of the Canadian government's response to the events of 11 September 2001 in the United States, we reported on deficiencies in intelligence management across the government, from setting priorities for intelligence to coordinating and sharing information between departments and agencies. We also found deficiencies in the assessment of lessons learned following critical incidents, in information and communications systems, in security screening for airport personnel, and in the use of watch lists and lookouts—lists of individuals considered a threat to Canada or of interest to intelligence organizations.

Exhibit 1.1 Intelligence departments and agencies are subject to varying levels of review

Department or agency	Review body	Review body function
Canadian Security Intelligence Service (CSIS)	• Inspector General • Security Intelligence Review Committee	• The Inspector General reports annually to the Minister of Public Safety on the activities of the service. • The Committee reports annually to Parliament through the Minister of Public Safety on the operational performance of the Service and any complaints against CSIS.
Royal Canadian Mounted Police (RCMP)	• Commission for Public Complaints Against the RCMP • The courts review RCMP investigative processes when hearing criminal cases.	• Reports annually to Parliament on investigations of complaints received from the public. • May permanently limit or strike down statutory or common law powers. May review behaviour in individual cases.
National Defence	No separate review body. When assisting a federal agency, National Defence would be subject to that agency's review process.	N/A
Communications Security Establishment Canada	• Commissioner of the Communications Security Establishment Canada	• Reports to the Minister of National Defence annually, and to the Attorney General on any activity the Commissioner believes may not be in compliance with the law. The Minister tables the report in Parliament.
Canada Border Services Agency	No separate review body	N/A
Foreign Affairs and International Trade Canada	No separate review body	N/A
Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	No separate review body	• *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* provides for review of the operation of the Act every five years. • The Privacy Commissioner can review and report to Parliament every two years on the measures taken by FINTRAC to protect information it receives or collects.

Note: All departments and agencies listed are subject to review by the Privacy Commissioner, the Information Commissioner, the Human Rights Commissioner, and the Auditor General.

Events since our previous audits

1.5 Since our 2003 and 2004 audits, there have been a number of commissions of inquiry that have examined and, for those that have reported their findings, made recommendations on the use of intelligence and how it is shared, either between departments or with other countries. The inquiries are the following:

- Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar
- Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin
- Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

In addition, the Minister of Public Safety mandated a Task Force on Governance and Cultural Change in the Royal Canadian Mounted Police to examine, among other things, the RCMP management structure, accountability, and oversight.

1.6 For the most part, the two inquiries into the actions of Canadian officials concluded that information needs to be shared to protect Canada's national security. However, any information shared should include a reference to its level of reliability and to whom the information may be transmitted. Information sharing was a central theme of the terms of reference of the Air India inquiry; however, the final report had not been released at the time of our audit.

1.7 Finally, the report of the Task Force on Governance and Cultural Change in the Royal Canadian Mounted Police, released in December 2007, contained recommendations to consider a form of oversight of the RCMP. However, at the time of this audit, the government had not announced any plans to implement these recommendations.

Focus of the audit

1.8 This follow-up audit assessed the progress that the government has made in implementing the recommendation from Chapter 10 of our November 2003 Report, Other Audit Observations, regarding independent reviews of security and intelligence agencies, and selected recommendations on intelligence and information sharing from our March 2004 Report, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative.

1.9 The departments, agencies, and review bodies included in this follow-up audit are the same as those included in our original audits.

1.10 More information on the objective, scope, approach, and criteria can be found in **About the Audit** at the end of this chapter.

Observations and Recommendations

Independent review of intelligence agencies

Departments and agencies have assessed the level of review of intelligence agencies

1.11 In 2003, we examined the level of independent review in place for each agency with the power to collect intelligence on Canadian citizens. Both the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) exercised similar powers of intrusion for reasons of national security when authorized by the courts. While CSIS had a relatively strong external review regime, the RCMP did not. The Commission for Public Complaints against the RCMP (CPC) could investigate only specific complaints or occurrences, and it could receive only information that the RCMP Commissioner thought relevant. The CPC could not perform audits on policy or systemic issues.

1.12 We reported in 2003 that the Commissioner of Communications Security Establishment Canada (CSEC) had full powers to review the work of CSEC and report what he found to Parliament and the Attorney General. Some agencies involved in security intelligence or enforcement, such as the Canadian Forces and Canada Border Services Agency (CBSA), were not subject to independent review by a body with a specific mandate to review security intelligence activities.

1.13 Subsequent to our audit, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar revealed serious weaknesses in the management control of both the RCMP's National Security Criminal Investigations program and its related external review regime. The commission report made detailed recommendations on strengthening the external review regime for all agencies. The Chair of the CPC has also made public proposals for improving the review framework, as has the Task Force on Governance and Cultural Change in the RCMP.

1.14 The work done by these subsequent inquiries and other reports has pointed out several additional problems to those identified in our 2003 audit report:

- Because the external review agencies have a mandate to review only single agencies, but more and more security work is done by joint task forces, there is an increased potential for review agencies to be unable to access the entire record of an investigation.
- At the RCMP, events in recent years have resulted in internal and public inquiries calling for more extensive external review of regular policing, which could decrease the need for special inquiries.
- In his annual report, the CSEC Commissioner qualified his opinion that CSEC is acting lawfully by saying he believes that there are ambiguities in CSEC's legislation; however, the report does not provide any details nor does it clarify the implications of this issue. Since the CSEC Commissioner's primary role is to determine the lawfulness of CSEC activities, the implications of this qualified opinion are serious. Both the House of Commons subcommittee and the special Senate committee on the review of the *Anti-terrorism Act* called on the CSEC Commissioner and the government to resolve their different positions on the legislation. CSEC is working with the Department of Justice Canada to address these issues through proposed legislative amendments.

1.15 Public Safety Canada, with the assistance of other departments, took the lead in coordinating an assessment of the level of independent review of intelligence agencies. Public Safety Canada is in the process of suggesting changes to the external review of these agencies. As part of this review, Public Safety Canada completed background papers that recognized the perceived lack of effectiveness of the CPC, the lack of interagency review capacity, the absence of independent review for some national security activities, and the lack of a clear role for parliamentarians in national security review.

1.16 The background papers also state several principles for an improved review model, including ensuring accountability, public confidence, and operational effectiveness. The papers also recommend that the level of review be proportionate to the level of intrusion and that reviews look beyond individual agencies to reflect the integrated nature of national security activities. If these proposals are implemented, they would address our 2003 recommendation. At this

point, no decision has been taken, nor is the timing of any planned implementation known.

1.17 While the government is not ready to implement corrective action on the level of independent review of security and intelligence agencies, two of the key agencies—the RCMP and Department of National Defence—have improved internal controls of their intelligence functions, as described in Exhibit 1.2.

Exhibit 1.2 Two key organizations have improved internal controls of intelligence functions

The Royal Canadian Mounted Police (RCMP) has taken action to better control its national security investigations. An RCMP internal audit published in July 2007 found that the RCMP's national security criminal investigations were not always in compliance with policy and ministerial direction. RCMP headquarters was not aware of all national security investigations and monitored only some of those of which it was aware.

The RCMP has improved its management of its national security operations, as its National Security Operations Branch now oversees all national security criminal investigations, from start to finish, to ensure that they comply with government and RCMP policies. The role of this new unit is to provide assistance to field units and ensure that investigations adhere to the RCMP principles on how to manage major cases.

In addition, National Defence and the Canadian Forces have made significant progress in integrating the intelligence functions that were formerly scattered across National Defence and the Canadian Forces, both domestically and overseas, under a single Chief of Defence Intelligence. This has created one of the largest intelligence capabilities in the government and has improved the internal control of defence intelligence.

At the time of our audit, there was no dedicated independent review of National Defence's intelligence functions. However, when operating in support of other agencies in Canada (such as the RCMP, the Canadian Security Intelligence Service, and Communications Security Establishment Canada), defence intelligence activities may be subject to the bodies that review those agencies.

1.18 Even though major inquiries have been held and considerable preparatory work has been done on the external review of national security agencies, no decisions have been taken to ensure that agencies are subject to a level of review proportionate to their intrusive powers. However, progress is seen as satisfactory because the government has completed its assessment (Exhibit 1.3).

Exhibit 1.3 Progress in addressing our recommendation on the level of agency review

November 2003 Report of the Auditor General of Canada, Chapter 10	
Recommendation	**Progress**
The government should assess the level of review and reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion. (paragraph 10.162)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Management of security intelligence

Significant improvements have been made, but gaps remain

1.19 Our 2004 audit reviewed the management of security intelligence, finding that overall direction came from five high-level government committees within the intelligence community, and that decision making was by consensus. When agencies could not reach consensus, decisions could be delayed. We were unable to assess the decisions made regarding overall government security priorities because they were subject to ministerial and Cabinet confidences.

1.20 We observed that there was some redundancy in the organization and development of strategic intelligence and that there were inadequate formal systems to take action on tactical intelligence. Alerts were sometimes passed by informal personal networks and could be delayed or lost.

1.21 At the time of our 2004 audit, the government had begun to create national security units that integrate representatives of agencies in Canada and, where appropriate, the United States. These include the Integrated National Security Enforcement Teams (INSET) and Integrated Border Enforcement Teams (IBET), led by the Royal Canadian Mounted Police (RCMP), and the Integrated National Security Assessment Centre (INSAC), led by the Canadian Security Intelligence Service (CSIS). These national security units were not always functioning well. For example, not all relevant agencies were contributing staff to INSAC, and a memorandum of understanding between the RCMP and CSIS to share information had expired.

1.22 We also observed in 2004 that while officials of various departments and agencies had cited the *Privacy Act* as a reason for not exchanging information, they could not provide any legal opinions,

specific references to legislation, or judgments as a basis for that opinion. The government has taken a number of initiatives to respond to the 2004 findings.

1.23 In April 2004, the government published Canada's National Security Policy, which directly addressed several of the weaknesses reported in our 2004 audit. First and foremost, it underlined the intent to build an integrated security system based on common definitions and assigned roles and responsibilities. Second, it recognized that comprehensive threat assessment was necessary to support integrated decision making.

1.24 The INSAC has been replaced by the Integrated Threat Assessment Centre (ITAC), an organizational unit of CSIS. ITAC's objective is to produce comprehensive threat assessments and analyses that are distributed within the intelligence community, the private sector, and to emergency services. Intelligence reports are seen by users to be timely and relevant; however, there are still some questions about whether ITAC has sufficient resources and subject area expertise. A 2006 review of ITAC documentation conducted by the Security Intelligence Review Committee found that, for the most part, ITAC complied with the *Canadian Security Intelligence Service Act* as well as direction from the Minister.

1.25 Analysis of potential threats for significant events such as the 2010 Olympics are now being done by ITAC from the combined intelligence provided by the main departments and agencies involved in national security. This analysis is linked to the Government Operations Centre, the interdepartmental strategic-level operations centre that coordinates national responses to Canadian and global events. However, some officials told us that although the creation of ITAC is clearly a step in the right direction, the production of threat assessment within the government could still be improved.

1.26 The National Security Policy did not change the mandates of intelligence agencies or their management structure. However, the management structure has evolved and has been strengthened to include a committee of deputy ministers on national security and an intelligence subgroup of that committee. There are also committees of assistant deputy ministers on national security as well as on intelligence, and a committee of directors general on intelligence. In Canada, as is the case with most governments based on the British (Westminster) parliamentary system, there is no single executive authority below the Prime Minister managing national security issues. Each minister is accountable for the results of their departments and

agencies. If an issue cannot be resolved through consensus, it may be given different priority by different departments, or its resolution delayed until a decision can be reached at Cabinet or by the Prime Minister. The National Security Advisor advises the Prime Minister while the Deputy Minister of Public Safety advises the Minister of Public Safety. Both the National Security Advisor and the Deputy Minister of Public Safety believe that the current command structure meets the government's needs and is functioning well. Some Westminster-type governments have taken additional steps to integrate security programs, such as using a single, government-wide budget and integrated command structures for the management of security intelligence.

1.27 The current management structure of committees has not dealt with certain operational issues in a timely manner. While the ultimate decision rests with the appropriate department or agency, issues are normally moved forward only after consensus is reached by committees. We found that resolution of certain issues appeared to have been delayed by calling for certain departments to research the issue and report back, which could take months. The National Security Advisor felt that this amount of time was not excessive; as most items are quite complex and they are given their due priority.

1.28 In 2006, the RCMP and CSIS signed a new memorandum of understanding on information sharing, which resulted in the RCMP's adoption of CSIS priorities for counter-terrorism, the creation of a Joint Management Team for counter-terrorism work, and the participation in joint training. The RCMP believes that this has reduced the level of conflict of work between the agencies and improved the sharing of information.

1.29 Although one of the central principles of the National Security Policy is improved coordination and integration of security efforts among government agencies, we found a number of cases where there was a failure to achieve integration or to deal with problems efficiently and effectively.

1.30 One case occurred in the spring of 2007, when there was a potential incident on the East Coast. There was a dispute over the nature of the incident, whether it was a humanitarian, criminal, or a security issue. There was a breakdown of the government coordinating processes and a loss of operational communications security.

1.31 The government has fallen short on its National Security Policy vision for the new Marine Security Operations Centres (MSOCs).

Housed by National Defence and including the Canada Border Services Agency (CBSA), Transport Canada, the RCMP, and Canadian Coast Guard, the Atlantic and Pacific coast MSOCs were originally intended to have the authority and capacity to detect, assess, and respond to marine security threats. However, we found that the MSOCs have only a limited ability to combine and analyze data as departments do not have unrestricted access to each others' data due to legal constraints over information sharing. Moreover, while National Defence is responsible for housing the coastal MSOCs and providing services to the other departments, no department has operational authority over the other departments.

1.32 Transport Canada, the RCMP, and CBSA have not established adequate information sharing arrangements to address organized crime in major airports. We provide additional details in the section regarding security screening of airport personnel by Transport Canada (paragraphs 1.48 to 1.57).

1.33 The creation of the National Security Policy, along with the development of the Integrated Threat Assessment Centre and the strengthening of the management structure of security intelligence, went a long way in addressing our 2004 recommendation. However, while progress has been satisfactory (Exhibit 1.4), issues that cannot be resolved through consensus may be given different priority by different departments, or their resolution delayed.

Exhibit 1.4 Progress in addressing our recommendation on an integrated security policy

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.68)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

The government has conducted lessons-learned analyses

1.34 In our 2004 audit, we observed that it had taken about two years for the Assistant Deputy Minister Committee on Public Safety to follow up on the case of a Montréal resident caught attempting to smuggle explosives into the United States from Canada. Some agencies with principal involvement, such as the Passport Office, did not conduct any analysis.

1.35 We also observed in 2004 that, while the same committee had produced a lessons-learned report on the events of September 11, 2001, there had been no reporting of progress made against the report's recommendations. The only government-wide analysis conducted of the Government of Canada's response to those events was a four-page discussion paper for a meeting of agency heads that was prepared by the Interdepartmental Committee on Security and Intelligence. There were neither minutes kept of the meeting nor was there any resulting action plan.

1.36 As part of this follow-up audit, we reviewed several reports written by CBSA after the anticipated arrival of hundreds of illegal immigrants on the East Coast. No immigrants were discovered; however, one report noted that the operation encountered the same difficulties in coordination as the 1999 arrival of a large number of illegal immigrants on the West Coast. These findings need to be followed up on to ensure that lessons can be learned to better respond to similar future events.

1.37 We found that CSIS has a formal lessons-learned system to assess its operations. For example, it undertook a lessons learned report for a protest with potential for politically motivated violence. The exercise assessed how well CSIS was able to consolidate information coming in from a number of sites in Canada and prepare assessments for government managers.

1.38 Public Safety Canada has not completed its lessons-learned framework for federal departments and agencies, which it committed to completing in its response to our 2004 recommendation. It has, however, begun to develop a national framework for lessons learned, including other levels of government and non-governmental organizations. This initiative is in a very preliminary stage.

1.39 Public Safety Canada is the lead agency for coordinating the federal government's national program for security exercises, which it regards as a tool for incorporating lessons learned in operational practices and in diffusing them. It does not, however, track the

implementation of recommendations made in exercise reports. This is left up to the individual agencies.

1.40 The government has conducted lessons-learned exercises after significant security incidents. While these were not as comprehensive in some departments as we would expect, and there is no clear link to demonstrate that departments have integrated the changes in their operations, they are a step in the right direction (Exhibit 1.5).

Exhibit 1.5 Progress in addressing our recommendation on conducting a lessons-learned analysis

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.76)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

There has been little progress on balancing privacy with national security concerns

1.41 In 2004, we found that departments and agencies were not sharing intelligence information because of concern with violating provisions of the *Privacy Act* or the *Charter of Rights and Freedoms*, whether this concern was valid or not. While the Act appeared to accommodate sharing of information for national security reasons, departments and agencies could not support their interpretation of the law for not sharing information.

1.42 Since 2004, we have seen little progress on balancing privacy concerns with information sharing. The Treasury Board of Canada Secretariat collects annual reports from each department and agency that received new funding from the Public Security and Anti-Terrorism (PSAT) initiative. The annual reports contain a checklist of potential issues to bring to the attention of Treasury Board, including information sharing and legal issues. We reviewed these PSAT reports since the fiscal year 2004–05 and found 16 instances

where departments and agencies reported potential legal barriers to information sharing, including

- the "consistency of use" provision in the *Privacy Act* that requires that information be used only for the purpose for which it was collected, creating a potential barrier to sharing criminal intelligence;
- the *Customs Act*, s.107, being a potential barrier to Customs officials (now border services officers) sharing intelligence with other government departments;
- the inability of representatives from different departments and agencies to share intelligence within the Marine Security Operations Centres except within existing legal authorities; and
- significant challenges between Transport Canada and CBSA in sharing information in the Air Cargo Security Initiative due to differences in their mandates, priorities, and legal restrictions in the sharing of information.

1.43 The Department of Justice Canada provides advice to ensure departmental officials are well informed as to the legal need to protect information while protecting national security. The Department maintains a counter-terrorism desk book to ensure its lawyers provide consistent advice to departmental officials.

1.44 Justice Canada has been tasked by the deputy minister committee on national security, which includes representatives from Privy Council Office, Treasury Board of Canada Secretariat, and Public Safety Canada, to prepare an inventory of legal problems related to sharing of national security data. Justice Canada officials informed us that, in consultation with other departments, they determined that it would be more useful to describe legal problems on a thematic basis as a means of identifying potential solutions. Justice Canada is also working with the Interdepartmental Marine Security Working Group to identify potential barriers to information sharing and their possible resolution. Documents reviewed indicate that Justice Canada is aware of both the *Privacy Act* and *Customs Act* issues, as well as problems sharing data within the MSOCs. According to Justice Canada officials, information sharing problems may be due to the lack of shared or consistent mandates between departments and agencies and that one potential solution would be to amend their legislative mandates.

1.45 CBSA informed us that it is doing its own review of the authorities that govern all aspects of information sharing with partners. It is also seeking designation under the *Access to Information Act* and the *Privacy*

Act as an investigative body, which would allow it to receive and share information more easily with law enforcement agencies.

1.46 The government has begun to study certain aspects of the privacy issue raised by our 2004 recommendation, but has not realized any progress (Exhibit 1.6).

Exhibit 1.6 Progress in addressing our recommendation on balancing privacy with national security concerns

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.94)	**Unsatisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

1.47 Recommendation. The Privy Council Office and Public Safety Canada, with the assistance of the Department of Justice Canada and the Treasury Board of Canada Secretariat, should increase their efforts to examine and provide guidance on the sharing of information among government departments and agencies while balancing privacy concerns with national security concerns.

Government's response. The Government of Canada recognizes the importance of information sharing, both domestically and internationally, in ensuring the safety and security of Canadians. Within the Government of Canada, each department and agency undertakes information sharing in accordance with Canadian laws and their respective legislation, mandates, and regulations.

The Privy Council Office (PCO), Public Safety Canada, Treasury Board of Canada Secretariat (TBS), and Justice Canada agree that PCO and Public Safety, with the assistance of Justice Canada and TBS, will continue their efforts to examine and coordinate horizontal issues on the sharing of information among government departments and agencies while balancing privacy concerns with national security.

Privy Council Office's response. The Privy Council Office will help coordinate departments' collective efforts to develop policies related to sharing information with one another. Information sharing issues vary widely, reflecting the laws, mandates, and statutory requirements of individual departments; there is no single solution that will address all of them. As such, many information sharing issues must be managed on a case-by-case basis in conforming with specific mandates.

Public Safety Canada's response. Public Safety Canada is fully committed to working with other federal agencies and departments within a responsive and integrated national security policy framework to address future and current threats to our country. An integral part of this effort includes information sharing. Fundamental to our policy framework are the key Canadian values of democracy, human rights, and respect for the rule of law. It is therefore essential that privacy risks inherent in intra-institutional or cross-jurisdictional information sharing be properly identified, assessed, and resolved to ensure that the government not only strengthens our national security but continues to respect the privacy of individuals.

Department of Justice Canada's response. Justice Canada will continue to assist other departments by providing advice on the balance between the very real information sharing needs of the government and important values such as privacy and other human rights.

A recent Justice Canada initiative will identify obstacles within the current legal and policy framework that might inhibit the sharing of national security information. This review will be conducted with a view to developing principles to inform the government's approach to information sharing in the field of national security, and proposing for consideration by decision makers, administrative and legislative options to achieve information sharing objectives, while respecting the guiding principles.

Treasury Board of Canada Secretariat's response. The Treasury Board of Canada Secretariat (TBS) will continue efforts to share information while balancing privacy and national security concerns. It will assist departmental leads in these efforts by providing policy guidance and advice on matters relating to information management, privacy, and security. TBS is also committed to providing regular summary reports to Justice Canada and Public Safety Canada on issues related to information sharing and interoperability that are reported to TBS through the Public Security Initiatives Annual Reporting Process.

Systems to support information sharing

Sharing of information for security screening of individuals working at airports has not improved

1.48 Our 2004 audit found that some individuals who had been granted clearance to work in restricted areas of airports by Transport Canada had a criminal record; others were involved in criminal conspiracy, while still others had some association with known criminals. Transport Canada claimed that a section of the *Aeronautics Act* limits its ability to withhold a security pass only if it relates to "preventing unlawful interference with civil aviation" and that this interference is confined by international convention to such activities as hijacking and sabotage (Exhibit 1.7). Transport Canada also believed that the number of persons who should have security clearances withdrawn because of criminal association was very small.

Exhibit 1.7 Transport Canada's focus regarding aviation security is on the unlawful interference with civil aviation

Transport officials maintain that their only authority regarding aviation security is to prevent the "unlawful interference with civil aviation," which has been interpreted as physical threat to aircraft and passengers. Transport Canada officials agree that transporting drugs by concealing them in the aircraft could be considered unlawful interference. However, Transport Canada has not agreed that it has a role to prevent criminal organizations from infiltrating airports as it believes that its responsibility does not extend to preventing unlawful activity. Instead, Transport Canada believes that if it does prevent unlawful activity at airports as a result of its security screening process for airport workers, this may be a "side benefit."

Source: Transport Canada

1.49 At Transport Canada's request, the Royal Canadian Mounted Police (RCMP) reviewed the files of all existing passholders (125,926) shortly after our 2004 report. The RCMP identified only 73 individuals as requiring further investigation. Of those

- thirty-three were no longer working at an airport;
- nine were cases of mistaken identity;
- four had their clearances suspended as they had been arrested and charged but not yet convicted;
- one was denied a clearance because of association with organized crime;
- two had clearances cancelled but later reinstated on completion of a full investigation;
- one case was undetermined as to outcome; and

- twenty-three were considered not to be of interest to Transport Canada as they had been included in the Canadian Police Information Centre database because of suicidal tendencies, or were no longer of interest to the police or the RCMP.

1.50 The discrepancy between our 2004 results and those reported by Transport Canada is explained by our audit using all sources of RCMP criminal intelligence, while the Transport Canada review did not. Our audit examined a sample of about 400 files, for which the RCMP analyzed the criminal intelligence databases on our behalf. Transport Canada's comprehensive review included over 125,000 files as noted above, but searched other databases only if there was a known result from the first query. We believe the methodology used by Transport Canada accounts for the difference in the results.

1.51 Since its initial 2004 review, Transport Canada has implemented a new process requiring additional information when reviewing applications for a security pass from new or potential employees. Following this new process, it did not issue passes to 971 of 3,717 individuals as there was insufficient information available for the previous five years to make an assessment. The RCMP identified an additional 87 individuals requiring investigation. Of these, 22 were denied or had clearances revoked and 2 were pending. However, an RCMP high-level analysis of organized crime at eight of Canada's largest airports (Vancouver, Edmonton, Calgary, Winnipeg, Toronto, Ottawa, Montréal, and Halifax) released publicly in 2008 found that there were more than 60 airport employees with criminal links. Many organized crime groups were found working within or using these airports.

1.52 In addition, the RCMP may receive incomplete information on applicants from Transport Canada. Once a person has been identified as requiring further investigation, the RCMP requests a consent form from Transport Canada, but this is often provided with information on the applicant's spouse, ex-spouse, or common-law partner blacked out. While the RCMP regards this information as necessary to complete the assessment, Transport Canada believes that the *Privacy Act* prohibits the Department from releasing this information.

1.53 Conversely, the RCMP may not give full information to Transport Canada for two possible reasons. First, third-party providers of information, such as municipal police forces, have not given permission for their information to be fully released; second, some RCMP officials believe that Transport Canada will disclose police intelligence information to those questioning a denial or revocation of their security

clearance. However, the Department of Justice Canada representatives informed us that this should not prevent Transport Canada from receiving this information as it should protect all data received. In addition, the memorandum of understanding between the RCMP and Transport Canada regarding information sharing was terminated by the RCMP on 31 December 2007, as it no longer complied with ministerial direction or with the recommendations of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. Applicants who are denied a clearance are informed in writing that they may apply for a review to the Federal Court.

1.54 We also noted that Transport Canada has not developed criteria for reviewing applications for restricted area passes, but makes the decision whether to approve problematic applications on a case-by-case basis. For example, a person applying for security clearance may have a criminal record. However, there are no established criteria to differentiate between those posing an increased security risk and those who committed less serious offences that may have happened in the distant past.

1.55 We did not retest a sample of files as we did in 2004. However, we highlight one case where a pass had been granted to an individual who had assault and weapons convictions and was under investigation for a murder relating to drug smuggling at a large airport.

1.56 While Transport Canada conducted a comprehensive review of its clearance holders, this was not based on complete police information, and Transport Canada should place limited reliance on the work conducted. As a result, Transport Canada may be granting clearance to high-risk individuals for work in secure areas of Canada's airports. Progress on the sharing of information for the security screening of individuals working at airports is thus unsatisfactory (Exhibit 1.8)

1.57 **Recommendation.** While awaiting direction on the sharing of personal information, Transport Canada and the RCMP should increase efforts to share information on individuals who have applied for security clearance to work at airports. Transport Canada should clarify its criteria and procedures when granting security clearance to individuals with previous criminal links.

The RCMP and Transport Canada's response. Transport Canada and the Royal Canadian Mounted Police (RCMP) agree that they will continue their efforts to share information on individuals who have applied for security clearance to work at airports. Transport Canada

agrees that it will continue efforts to formalize criteria and procedures used for security clearance decisions.

Transport Canada and the RCMP are negotiating a new memorandum of understanding for the exchange of information relevant to transportation security clearances, including criminal intelligence. In the context of these negotiations, Transport Canada and the Royal Canadian Mounted Police are reviewing options to address privacy and information sharing concerns with a view to improving the comprehensiveness and reliability of information used in processing transportation security clearances. Further, Transport Canada is formalizing criteria and procedures to be used for security clearance decisions.

Exhibit 1.8 Progress in addressing our recommendations on holders of clearances to restricted areas at airports

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.154)	**Unsatisfactory**
Once it has obtained access to complete police information, Transport Canada should begin a comprehensive review of all clearance holders. (paragraph 3.155)	**Unsatisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Interoperability and information sharing need continued attention

Interoperability—the ability of the federal government's numerous security information systems to work together technically, legally, semantically (through standard terminology), and culturally (through the willingness of organizations to share information).

1.58 In our 2004 report, we found that the government had, following September 11, 2001, identified the need for increased interoperability between systems to reduce or eliminate the walls or barriers to information sharing that existed at that time. Examples of such barriers were the lack of coordination and systematic updating of watch lists (or lookouts) and the exclusion of lost or stolen passports from the lists. In response, an assistant deputy minister Interoperability Working Group was established to identify "quick hits" (immediate action) to improve information sharing related to national security. This working group had completed its interim report *Improving Interoperability and Data Exchange* in September 2002. Our audit noted that progress

achieved on the quick hits was not sustained. Only three projects were successfully completed, two projects had doubtful progress, and five projects made no progress since the Interoperability Working Group completed its interim report. We were informed by Treasury Board of Canada Secretariat and Public Safety Canada officials that, on further study, some remaining issues did not have short-term solutions and some had been combined with other issues.

1.59 Since 2004, the government has focused more attention on interoperability by working toward a national security information-sharing framework that would assist all departments. This framework, developed by Public Safety Canada, is reflected in its February 2008 report *Public Safety Interoperability—A Way Forward*.

1.60 The 2008 report was a conceptual strategy document designed to provide a foundation for future interoperability projects. However, it was never endorsed by the government, leaving its status in question. While this report proposes a foundation for future information sharing, it does not adequately identify the mechanisms needed by departments and agencies to achieve this goal.

1.61 Several of the original "quick hits" from the interoperability project were completed, and the government has concluded that others did not have short-term solutions, or have been combined with other issues. The 2008 report is a conceptual foundation document for a future interoperability project whose status remains uncertain at this date, and does not identify mechanisms to achieve information sharing (Exhibit 1.9).

Exhibit 1.9 Progress in addressing our recommendation on issues of interoperability and information sharing

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.84)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

The government is developing a communications system at the secret level

1.62 In 2004, we noted that another barrier to information sharing was the lack of a government-wide system allowing communication at the "secret" level among departments and agencies. A previously proposed system had been abandoned when it was found it could be vulnerable to attack. In November 2003, the government began developing a new communications system at the secret level.

1.63 Public Safety Canada is the lead on this project, and it obtained $30 million for the pilot stage. Communications Security Establishment Canada (CSEC) is the technical authority for the project. The new system is called the Secret Communications Interoperability Project (SCIP) and uses customized commercial products (except for the cryptographic equipment). An additional $8.4 million had been allocated to Public Safety Canada to establish a policy and legal framework for information sharing, which included the development of the previously mentioned report *Public Safety Interoperability—A Way Forward.* However, this policy and legal framework was not resolved before SCIP's development and pilot rollout.

1.64 To date, a data centre to host the SCIP has been built and the security put in place to protect it, and all necessary equipment has been installed. However, the limited implementation stage, which will include the RCMP, the Canadian Security Intelligence Service (CSIS), Public Safety Canada, the Canada Border Services Agency (CBSA), and possibly Foreign Affairs and International Trade Canada as participating partners, requires another $4.4 million to be completed. Public Safety Canada cannot estimate the cost to provide SCIP to all anticipated users as this will depend on the costs of different models. The number of expected users has decreased by 75 percent.

1.65 The data transmission for SCIP will use the Secure Channel network infrastructure, which provides operational cost savings. Participating departments are expected to contribute to operational costs, but will not pay for individual transactions. The design of SCIP relied on lessons learned from previous projects at CSEC, particularly the Classified Message Handling System. SCIP is currently more than a year behind its original schedule, but is expected to finish its pilot by the end of March 2009. Significant progress has been made toward finding a technically feasible and secure solution. While its success depends on obtaining additional funding and being adopted by its target users, Public Safety Canada and Treasury Board of Canada Secretariat remain confident that it will succeed.

1.66 Significant progress has been made in the development of the government-wide communications system at the secret level. However, it is still in the pilot stage, and its success is contingent upon receiving additional funding and user acceptance. While progress was slow to start, the project is complex and has experienced better progress recently (Exhibit 1.10).

Exhibit 1.10 Progress in addressing our recommendation on a government-wide communications system at the secret level

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.88)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

The RCMP has made improvements to its fingerprint systems

1.67 In 2004, we reported that the RCMP had an estimated 60,000 fingerprints waiting to be processed in 2003, triple the number from 2001. The Public Security and Anti-Terrorism (PSAT) initiative provided $38.6 million to improve the collection and analysis of fingerprints by using electronic machines to take digitized fingerprint images. Some 139 machines were installed. By January 2007, the RCMP reduced by 65 percent its backlog of fingerprints collected from individuals to be updated in their criminal records. However, this backlog subsequently rose by 50 percent. This was largely due to two factors: an increase in fingerprint analysts' workload because heightened security demands of many groups required additional fingerprint checks, and difficulties in attracting and retaining experienced analysts. At the time of our audit, performance data obtained from the RCMP indicated that the backlog of fingerprint checks had been eliminated, but a backlog still exists in updating this information in individuals' criminal records.

1.68 Our 2004 chapter reported that the electronic machines take and transmit fingerprints digitally, but the RCMP uses a manual system to analyze them and compare them with existing fingerprint data. The RCMP had proposed the Real Time Identification system (RTID) to

automate the process but at the time of our 2004 audit, it had not received funding for this project.

1.69 Funding has since been received for RTID, amounting to $90 million, and the RCMP allocated an additional $30 million from its own resources. The RCMP has indicated that the project is progressing well and is on budget. Waiting times for responses to requests for fingerprint checks have decreased significantly.

1.70 The RTID project began behind schedule in November 2006 and the first phase was completed in the summer of 2008, some 21 months later than the original project plan, due in part to delays in project approval and a more thorough review of the policy changes needed to implement RTID. The majority of the second and final phase is scheduled for completion in 2010.

1.71 While the RCMP has devoted additional resources and has eliminated the backlog for checking fingerprints against its database of existing fingerprints, a backlog remains in updating individuals' criminal record information. The RCMP has received funding for its RTID project and, while behind original timelines, is progressing toward implementation (Exhibit 1.11).

Exhibit 1.11 Progress in addressing our recommendations on improving the processing of fingerprints

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
The RCMP should find and implement a solution to deal with its fingerprint backlog. (paragraph 3.107)	**Satisfactory**
The RCMP and Public Safety and Emergency Preparedness Canada should give priority to implementing the Real Time Identification project. (paragraph 3.109)	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Coordination of information on lookouts has improved, but there is a gap in quality

1.72 Our 2004 report found that many of the processes supporting the use of watch lists or "lookouts" relied on manual, paper-based records and transfers of information. For the remainder of this report we will use the term lookouts to mean both lookouts and watch lists—lists of people who are to be prevented from entering Canada or whose entrance is to be monitored by Canadian border services officers. The

report noted missing terrorist lookouts, duplication of records, classification errors that could result in inappropriate decisions regarding individuals entering Canada, and names listed on lookouts that should have been already removed. Border lookouts did not contain a list of lost or stolen passports, but this information was provided to the RCMP with a substantial backlog of data that needed to be manually entered into its database. Lastly, there was no system to transfer passport information from the RCMP to the border lookouts.

1.73 Since our audit, while there is no ongoing formal mechanism to address national security lookout coordination, there is better coordination of information transfers on lookouts between organizations. The nature of lookouts may be long-term, where there is a known individual who is to be prevented entry at any time in the future, or short-term, where there is specific information that an individual may try to enter Canada in the near future.

1.74 The individual lookout information CBSA uses comes from various intelligence and law enforcement agencies, and is received in the form of either electronic transfers of data or other forms of communication. For example, CSIS data on long-term lookouts are electronically transmitted on a weekly basis to Citizenship and Immigration Canada (CIC) and CBSA. These lookout data records are updated as new information is received and reviewed every two years to remove entries that no longer apply. Short-term lookouts are provided to CBSA by memorandum, which are then entered manually into CBSA's systems.

1.75 The RCMP and CBSA work together as part of Integrated National Security Enforcement Teams, where information is strictly controlled and transferred only as needed on a case-by-case basis. In addition, the RCMP and CBSA have jointly undertaken work to develop a glossary of common terminology. The RCMP continues to provide INTERPOL information to CBSA for lookouts and expects that this process will be automated in 2009. However, legislative requirements of the *Customs Act* and *Privacy Act* restrict the sharing of some information that CBSA may have on international fugitives or criminals with the RCMP and thence to INTERPOL. RCMP officials believe that Canada's inability to provide information to INTERPOL may jeopardize the level of foreign assistance we receive.

1.76 Coordination among various agencies is also needed in using passenger information collected from airlines, as required by federal law since late 2001, to help federal agencies assess the risks presented by travellers before they arrive in Canada. The RCMP, CSIS, Passport

Canada, and CBSA cooperate as permitted by current legislation in managing and coordinating the use of advance passenger information (API), collected when passengers check in, and passenger name record (PNR) data, which is drawn from airline flight reservation systems.

1.77 There was also progress in improving the management and coordination of lookouts when CBSA was granted full access to the Canadian Police Information Centre database, which contains stolen passport information. CBSA can now match API and PNR data against all arrest warrants contained in this database, including offences that could be associated with threats to national security and immigration warrants, but only to identify persons involved with or connected to terrorism or other serious crimes, including organized crime, that are transnational in nature.

1.78 In addition, Transport Canada maintains a list of individuals who pose a threat to aviation security, named the Specified Persons List, which is based on information received from the airlines, CSIS, and the RCMP, and communicated with the airlines. Transport Canada is not permitted to share this information with any other agencies nor can other agencies contribute to this database.

1.79 For quality, lookouts need to be accurate, comply with legislation and regulations, and be regularly reviewed and updated in a timely manner or have information deleted when no longer relevant to national security uses. In addition, any errors need to be noted and investigated, resulting in the correction of processes and data records.

1.80 The Canada Border Services Agency told us that the agencies contributing national security data to its lookout databases are each responsible for ensuring the quality of the data provided. CBSA officers regularly review CBSA originated national security lookout data. However, there are no formal agency-wide data quality procedures for information provided by other agencies. As a result, lookout information provided by other agencies and contained in CBSA databases is not available for review by those agencies to ensure that it has been entered accurately and is still valid.

1.81 There has been substantial progress in the electronic exchange of lookout information since our 2004 report, which has led to some improvements. However, there is no ongoing formal mechanism to address national security coordination of lookouts. Processes to ensure the quality of lookouts have improved in certain areas; however, there is a gap in ensuring the quality of lookout information provided to CBSA by other agencies (Exhibit 1.12).

Exhibit 1.12 Progress in addressing our recommendation on the coordination of lookouts and on the quality of lookouts

March 2004 Report of the Auditor General of Canada, Chapter 3	
Recommendation	**Progress**
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. (paragraph 3.133)	**Satisfactory**
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. (paragraph 3.134)	**Unsatisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

1.82 Recommendation. The Canada Border Services Agency, with the assistance of other agencies providing lookout information, should develop processes to ensure that the information used by CBSA is accurate and valid.

Canada Border Services Agency's response. The Canada Border Services Agency (CBSA) agrees. The Agency will examine this recommendation in consultation with partner agencies to identify gaps and possible measures to enhance the accuracy and validity of lookouts originating from the CBSA's partners. In the long term, CBSA will examine the possibility of automating its lookout interfaces with partners.

Conclusion

1.83 The federal government has made satisfactory progress in implementing our 2003 recommendation to assess the level of review and reporting to Parliament for security and intelligence agencies. However, much work remains. While the government has completed its assessment of the level of independent review of security and intelligence agencies, it awaits the final report of the Air India Inquiry before proceeding with its proposals. As a result, the situation remains unchanged since our 2003 report.

1.84 The federal government has made satisfactory progress in implementing several selected recommendations from our 2004 chapter in the management of security intelligence and the sharing of information among security and intelligence agencies. We found significant progress with the creation of Canada's National Security Policy and in the organization and coordination of priorities among federal departments and agencies involved in security issues. The government has conducted lessons learned exercises after significant security incidents to be better prepared for future events. The Royal Canadian Mounted Police (RCMP) also cleared its backlog of analyzing fingerprints and is progressing in its development of a computerized system to analyze digitized fingerprints. The government also took measures to improve the coordination of lookouts of individuals considered of interest to intelligence organizations.

1.85 Progress is slow, but satisfactory, in the area of developing systems that allow the sharing of intelligence information. The government-wide communications system at the secret level has progressed to a limited implementation stage and is contingent upon additional funding and user acceptance.

1.86 However, for other recommendations, there was either little or no progress or it was slow. Gaps remain in the coordination and integration of security efforts among government agencies, where we found a number of cases where there was a failure to achieve integration or to deal with problems efficiently and effectively. We found 16 instances where departments and agencies have reported legal barriers to information sharing. The government has not completed its research into, nor provided consistent guidance to departments on, managing the balance between the privacy of individuals and requirements to maintain the security of the nation. This has led to poor sharing of information among government departments.

1.87 Transport Canada and the RCMP are still not sharing criminal intelligence information effectively. While they have a memorandum of understanding for conducting security clearances of individuals working at airports, the process does not include checking against all criminal intelligence databanks. Transport Canada may be granting clearance for access to restricted areas at airports to high-risk individuals with criminal links.

1.88 Processes to ensure the quality of information in lookouts have improved in certain areas; however, there is a gap in ensuring the quality of lookout information provided to CBSA by other agencies.

About the Audit

Objective

Our objective was to determine whether the government has made satisfactory progress in implementing the recommendation from the section "Independent reviews of security and intelligence agencies," in our November 2003 Report, Chapter 10, Other Audit Observations, and selected recommendations from the March 2004 Report, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative.

Scope and approach

The scope for this follow-up audit was to determine if satisfactory progress has been made concerning our 2003 and 2004 recommendations in the period from March 2004 to September 2008.

We examined the same departments, agencies, and review bodies that were included in the scope of our original audit and audit observations, adjusted to reflect government reorganizations: Privy Council Office, Public Safety Canada, Transport Canada, Canadian Security Intelligence Service, National Defence, Communications Security Establishment Canada, Royal Canadian Mounted Police, Foreign Affairs and International Trade Canada, Department of Justice Canada, Treasury Board of Canada Secretariat, Canada Border Services Agency, Citizenship and Immigration Canada, Passport Canada, Financial Transactions and Reports Analysis Centre of Canada, Security Intelligence Review Committee, Commission for Public Complaints Against the RCMP, and the Office of the Communications Security Establishment Commissioner.

Criteria

Listed below are the criteria that were used to conduct this audit and their sources.

Criteria	Sources
The government should assess the level of review and reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion.	November 2003 Report of the Auditor General of Canada, Chapter 10, Other Audit Observations, "Independent reviews of security and intelligence agencies," recommendation 10.162.
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.68.
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.76.

Criteria	Sources
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.94.
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.154.
Once it has obtained access to complete police information, Transport Canada should begin a comprehensive review of all clearance holders.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.155.
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.84.
Public Safety and Emergency Preparedness Canada and the National Security Advisor, with the assistance of the Treasury Board Secretariat, should coordinate and oversee the implementation of a government-wide communications system at the secret level.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.88.
• The RCMP should find and implement a solution to deal with its fingerprint backlog. • The RCMP and Public Safety and Emergency Preparedness Canada should give priority to implementing the Real Time Identification project.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendations 3.107 and 3.109.
The RCMP, the Canadian Security Intelligence Service, the Canada Border Services Agency, and the Passport Office should improve their management and coordination of watch-listing efforts that collectively contribute to Canada's national security.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.133.
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.	March 2004 Report of the Auditor General of Canada, Chapter 3, National Security in Canada—The 2001 Anti-Terrorism Initiative, recommendation 3.134.

Audit work completed

Audit work for this chapter was substantially completed on 25 September 2008.

Audit team

Assistant Auditors General: Wendy Loschiuk, Hugh McRoberts
Principal: Gordon Stock

Maryanna Basic
Steven Mariani
Donna Winslow

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

Appendix List of recommendations

The following is a list of recommendations found in Chapter 1. The number in front of the recommendation indicates the paragraph where it appears in the chapter. The numbers in parentheses indicate the paragraphs where the topic is discussed.

Recommendation	Response
Management of security intelligence	
1.47 The Privy Council Office and Public Safety Canada, with the assistance of the Department of Justice Canada and the Treasury Board of Canada Secretariat, should increase their efforts to examine and provide guidance on the sharing of information among government departments and agencies while balancing privacy concerns with national security concerns. **(1.41–1.46)**	**Government's response.** The Government of Canada recognizes the importance of information sharing, both domestically and internationally, in ensuring the safety and security of Canadians. Within the Government of Canada, each department and agency undertakes information sharing in accordance with Canadian laws and their respective legislation, mandates, and regulations. The Privy Council Office (PCO), Public Safety Canada, Treasury Board of Canada Secretariat (TBS), and Justice Canada agree that PCO and Public Safety, with the assistance of Justice Canada and TBS, will continue their efforts to examine and coordinate horizontal issues on the sharing of information among government departments and agencies while balancing privacy concerns with national security. **Privy Council Office's response.** The Privy Council Office will help coordinate departments' collective efforts to develop policies related to sharing information with one another. Information sharing issues vary widely, reflecting the laws, mandates, and statutory requirements of individual departments; there is no single solution that will address all of them. As such, many information sharing issues must be managed on a case-by-case basis in conforming with specific mandates. **Public Safety Canada's response.** Public Safety Canada is fully committed to working with other federal agencies and departments within a responsive and integrated national security policy framework to address future and current threats to our country. An integral part of this effort includes information sharing. Fundamental to our policy framework are the key Canadian values of democracy, human rights, and respect for the rule of law. It is therefore essential that privacy risks inherent in intra-institutional or cross-jurisdictional information sharing be

Recommendation	Response
	properly identified, assessed, and resolved to ensure that the government not only strengthens our national security but continues to respect the privacy of individuals. **Department of Justice Canada's response.** Justice Canada will continue to assist other departments by providing advice on the balance between the very real information sharing needs of the government and important values such as privacy and other human rights. A recent Justice Canada initiative will identify obstacles within the current legal and policy framework that might inhibit the sharing of national security information. This review will be conducted with a view to developing principles to inform the government's approach to information sharing in the field of national security, and proposing for consideration by decision makers, administrative and legislative options to achieve information sharing objectives, while respecting the guiding principles. **Treasury Board of Canada Secretariat's response.** The Treasury Board of Canada Secretariat (TBS) will continue efforts to share information while balancing privacy and national security concerns. It will assist departmental leads in these efforts by providing policy guidance and advice on matters relating to information management, privacy, and security. TBS is also committed to providing regular summary reports to Justice Canada and Public Safety Canada on issues related to information sharing and interoperability that are reported to TBS through the Public Security Initiatives Annual Reporting Process.

Recommendation	Response
Systems to support information sharing	
1.57 While awaiting direction on the sharing of personal information, Transport Canada and the RCMP should increase efforts to share information on individuals who have applied for security clearance to work at airports. Transport Canada should clarify its criteria and procedures when granting security clearance to individuals with previous criminal links. **(1.48–1.56)**	**The RCMP and Transport Canada's response.** Transport Canada and the Royal Mounted Canadian Police (RCMP) agree that they will continue their efforts to share information on individuals who have applied for security clearance to work at airports. Transport Canada agrees that it will continue efforts to formalize criteria and procedures used for security clearance decisions. Transport Canada and the RCMP are negotiating a new memorandum of understanding for the exchange of information relevant to transportation security clearances, including criminal intelligence. In the context of these negotiations, Transport Canada and the Royal Canadian Mounted Police are reviewing options to address privacy and information sharing concerns with a view to improving the comprehensiveness and reliability of information used in processing transportation security clearances. Further, Transport Canada is formalizing criteria and procedures to be used for security clearance decisions.
1.82 The Canada Border Services Agency, with the assistance of other agencies providing lookout information, should develop processes to ensure that the information used by CBSA is accurate and valid. **(1.72–1.81)**	**Canada Border Services Agency's response.** The Canada Border Services Agency (CBSA) agrees. The Agency will examine this recommendation in consultation with partner agencies to identify gaps and possible measures to enhance the accuracy and validity of lookouts originating from the CBSA's partners. In the long term, CBSA will examine the possibility of automating its lookout interfaces with partners.

Status Report of the Auditor General of Canada to the House of Commons—2009

Main Table of Contents